2013

Air Force NetCentric Operations Infrastructure and Solution Acquisition Guide

Version 1.0

17 October, 2013

Table of Contents

Air Force NetCentric Operations (NetOps) Infrastructure and Solution Acquisition Guide

1 Purpose

The purpose of the AF NetCentric Operations Infrastructure and Solution Acquisition Guide is to provide interim guidance for the purchase of solutions to support network operations, core enterprise services, and infrastructure development and operations including legacy Telephony. This guide provides policies, templates, and standards that govern the acquisition of NetCentric Operations Infrastructure and Solution services. It should be used to develop requirement packages to help ensure that all netcentric standards and compliance areas are conformed to.

2 How to Order

Users who have requirements that fall within one of the categories identified in paragraph 3 below will need to start by completing Appendix N1 - Network Operations and Infrastructure Solutions Checklist in order to put together the most complete requirements package and avoid any unnecessary delays in delivering services to the warfighter. Also, ensure you are in compliance with guidance issued by the AF CIO in paragraph 4 below.

The required documents and supplementary PWS templates are to be completed and submitted to your local Contracting Officer (CO) for final approval. Those documents and templates are easily identifiable and linked in the Table of Contents above.

3 Scope

This acquisition guide only provides guidance to the following Network Operations and Infrastructure Solutions categories:

- **Network Centric Services**

  Infrastructure, Infrastructure as a Services, Platform as a Services, Network Management, Development, O&M, Acquisition, Integration, System Engineering, System Upgrades, Test, Deployment, Sustainment, Production, Research, Command, Control, Communications, Computers (C4), Intelligence, Surveillance, Software Support, Reconnaissance (ISR) mission capabilities, Security, Information Assurance Architecture, Information Assurance Services, Voice, Video/Data, Enclaves, Federation, Enterprise Messing and Discovery Services, Help Desk, GIG Network Defense (GND), Enterprise Management and emerging technologies.

- **Data**

  Metadata Environments Services, MDE Infrastructure, MDE Lifecycle Management, Data Management, Software as a Service, Platform as a Service, Data Integration, Federation, Data Storage, Versioning, Indexing, Data Protection, Data Acquisition, Data Analysis, Data Farming, Data Integrity, Data Maintenance, Data Mining, Data Modeling, Data processing, Data Warehouse, Database Management, and Data Archiving.

4 Obligation of Funds for Data Servers and Data Centers

4.1 Federal Data Center Consolidation Initiative (FDCCI)

On 18 Aug 2013, the AF CIO signed a memorandum to change AFI 33-150, *Management of Cyberspace Support Activities,* in response to the DoD CIO's initiative to reduce the footprint of data centers within DoD.

4.1.1 Definition of Data Center

The Office of Management and Budget (OMB) defines a data center as a closet, room, floor or building for the storage, management, and dissemination of data and information.

4.1.2 Restrictions on Acquisition of Products and Data Center Upgrades

The AF CIO memorandum restricts the obligation of any and all funds to construct or modify existing data center buildings, facilities, or room; or acquire products in the below listed categories.

4.2 Products Requiring DoD CIO Approval

The below listed products cannot be acquired for use in data centers without DoD CIO approval:

- Servers of any type
- Server software of any type
- Storage to include Storage Area Networks (SAN), Network Attached Storage (NAS) and Direct Attached Storage (DAS)
- Racks
- Uninterruptable Power Supply (UPS)
- Routers, switches, etc. (unless specifically approved by AFLCMC/A3I as an AFNET asset)
- Cooling systems and environmental monitoring capabilities
- Backup capabilities, regardless of medium

4.2.1 Products Requiring AF CIO approval:

- End user devices (e.g., desktops, laptops, tablets, mobile devices), and associated software and services
- Service, support and maintenance contracts (e.g., warranty support, preventive, routine and emergency maintenance) for existing data center capabilities
- Replacement of casualty items
- Tactical/Mobile Processing Nodes as defined in the DoD CIO Core Data Center Reference Architecture

4.3 Exception to AFI 31-150

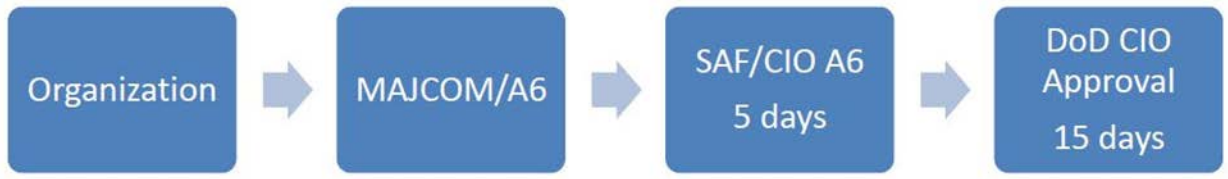
The following types of items are excluded from AF Data Center Infrastructure Management and this approval process (no other waivers authorized) per the 9 May 2013 DoD CIO memo.

- National Intelligence Program
- High Performance Computing Modernization Program (HPCMP)

4.4 Acquisition Approval Process

Data centers approvals from the DoD or AF CIO will be obtained through the Cyberspace Infrastructure Planning System (CIPS). Follow the guidance in Air Force Guidance Memorandum to AFI 33-150, *Management of Cyberspace Support Activities* found at http://www.safcioa6.af.mil/shared/media/document/AFD-130820-012.pdf

The approval process and approval time is depicted below in accordance with the aforementioned memorandum.



5 Points of Contact – Customer Support (CS)

E-mail CS at netcents@gunter.af.mil if you have specific questions in regards to this document. Please ensure "NetCentric NetOps Acquisition Guide" is noted in the subject line for review and appropriate distribution.

If you require immediate assistance, the CS can be reached at DSN 596-5070 option 1.

Appendix N1 NetOps and Infrastructure Solutions Solicitation Requirement Package Checklist

Instructions: Use this checklist to complete your requirement package. Submit the completed checklist and the other applicable documents to your local contracting officer to continue the Solicitation process.

#	DOCUMENTATION	REFERENCE	Check if complete. Answer Yes/No/NA Where Applicable
1.	**SOLICITATION INFORMATION**		
a.	Agency/Department: Organization Office Symbol: Organization Address:		□
b.	Solicitation Title: Brief Description:		□
c.	Customer Requiring Activity Primary POC Name: Title: Email: Phone: Secondary POC Name: Title: Email: Phone:		□
d.	Provide a Period of Performance:		□
4.	**MARKET RESEARCH**		
	Provide market research to support acquisition decisions. If needed, a Market Research Report template is provided.	N4: Market Research Report Template	□
5.	**ACQUISITION PLANNING**		

#	DOCUMENTATION	REFERENCE	Check if complete. Answer Yes/No/NA Where Applicable
a.	If an approved Acquisition Plan is available, submit for background information only.	FAR 7.103 – 7.107 AFFARS 5307.104 – 92(b)(3)	□
b.	Provide Acquisition Strategy Panel (ASP) Briefing Charts and ASP Minutes, if applicable.	AFFARS 5307.104 – 90	□
7.	SERVICES DESIGNATED OFFICIAL (SDO)		
	If required the Customer may appoint a SDO in accordance with AFI 63-101 as it states.	http://www.fas.org/irp/doddir/usaf/31-601.pdf	□
8.	QUALITY ASSURANCE		
a.	If needed, a COR Designation Template is provided for reference.	COR Appointment Letter Template	□
b.	Provide a copy of the COR's Phase 1 Training Certificate if needed.	OUSD (AT&L) Memo, 29 Mar 2010	□
c.	If needed, provide a Quality Assurance Surveillance Plan (QASP). If needed, QASP Templates are provided for reference.	N5: QASP Template	□
9.	REQUIREMENTS		
a..	Is this a Sole Source Solicitation? Contractor:	FAR 6.302 FAR 8.405-6	□

#	DOCUMENTATION	REFERENCE	Check if complete. Answer Yes/No/NA Where Applicable
b.	If this is a Sole Source, provide Justification for a Fair Opportunity Exception (FOE). If Justification is approved, use the appropriate FOE Coordination & Approval template, which is based on the Solicitation amount. If needed, Justification and Coordination & Approval templates are provided for reference.	N6: FOE Justification Template N7: FOE Coordination & Approval Templates FAR 6.303 FAR 16.505(b)(2)	□
c.	Complete the PWS Template	N2: Network Operations and Infrastructure Solutions PWS Template	□
d.	If classified information necessitates contractual security specifications, complete and include a DD 254.	N8: DD Form 254 Guidance AFI 31-601, Chapter 4	□
e.	Are there any supplementary attachments that need to be provided (i.e., network topology, building lists)?		□Yes □No □N/A
f.	Are there any requirements which are Mission Essential Requirements? If yes, they must be identified as such.	DoDI 3020.37	□Yes □No □N/A
g.	Since services are being required, determination must be made by the Program Office certifying that no Inherently Governmental Functions (IGF) are being accomplished by the Contractor. If needed, an IGF Memo template is provided.	N9: IGF Memo Template	□Yes □No □N/A
h.	Will there be Government Furnished Property (GFP) and Space? If yes, the Customer must provide a statement that the GFP or space is available. If needed, a template is provided.	N10: GFP D&F Template	□

#	DOCUMENTATION	REFERENCE	Check if complete. Answer Yes/No/NA Where Applicable
i.	Are there any consolidated contract requirements, that are, two or more requirements previously acquired separately now consolidated into a single requirement? If yes, provide justification. Applicable to actions greater than $5M.	DFARS 207.170-2 AFFARS 5307.170-3	□ Yes □ No □N/A
j.	Is this a new start program/project? If yes, the Customer must provide supporting file documentation, including appropriate congressional notification/approvals.	N11: New Start Validation Template□	□Yes □No □N/A
10.	INDEPENDENT GOVERNMENT COST ESTIMATE (IGCE)		
	Provide Independent Government Cost Estimate (IGCE) to include costs for option years. If needed an IGCE Template is provided.	N12: IGCE	□
11.	SOLICITATION AWARD EVALUATION		
a.	Provide the Evaluation Guidelines to outline selection criteria for Solicitation award, which the ordering CO will approve. If needed an Evaluation Guideline Template is provided.	N13: Evaluation Guidelines	□
12.	FUNDING DOCUMENTS		
a.	Provide funding documents (i.e., MIPR, PR, etc.) and ensure sufficient funds are available for the effort and funding appropriation properly matches the services being procured.	FAR 32.702 DFARS 204.7103 DoD 7000.14R	□
b.	Are the services being requested **severable or non-severable?** Severable services cannot exceed one year.	DoD 7000.14R, Vol. III, Chapter 8	□Yes □No □N/A

#	DOCUMENTATION	REFERENCE	Check if complete. Answer Yes/No/NA Where Applicable
c.	Confirm within 5 days of contract award, the Wide Area Workflow Inspector Code.	DFARS 252.232-7003	□
13.	CLIN STRUCTURE AND PRICING		
	Provide a CLIN Pricing Structure		□
14.	OZONE DEPLETING SUBSTANCE (ODS)		
	The Customer must provide either a certification that there is no Class I ODS or a copy of the GO / SES approval for use of Class I ODS.	N14: Ozone Depleting Substance Certificate Template□	□
16.	SOLICITATION POST AWARD TASKS		
a.	**Public Disclosure of Information** Does the PWS contain information that, if released, would be harmful to the government? FOIA Coordinator Name: E-mail: Physical Address:		□Yes □No □N/A

Appendix N2 Network Operations (NetOps) and Infrastructure Full and Open Solicitation Template PWS

[Requesting Agency Solicitation Title]

1. Purpose

[This paragraph should define the overall purpose and objectives of the contract]

2. Scope

[In this paragraph, summarize the specific type(s) of support your organization/program office is seeking and who the work supports (what organization(s) or domains). Do not go into too much detail, as this will be detailed under the "requirements" paragraphs that follow.]

3. Requirement / Description of Services

[The Description of Services describes at a high level (big picture) the services required under the contract, not each specific task. It should be consistent with the outcomes in the Services Summary and linked to Air Force/organizational requirements. The objective is to state, using established industry/government standards, what we need (objective), not how we need each task accomplished (methodology). The following is a list of the services/requirements on the NetOps ID/IQ contract. They can be modified as needed to meet Solicitation requirements. Sections 3.1-3.5 are example requirements that will help you facilitate the development of your PWS.

IMPORTANT--Describe the end product or outcome you want but avoid telling the contractor how you want it done.] **[Delete those that do not apply.]**

3.1.1. Implementation and Operation

3.1.2. Infrastructure Management

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

- Infrastructure Management shall support all AF mission requirements, and share data through federation with other infrastructure environments across the DoD, Federal agencies, and Joint and Coalition environments. The contractor shall provide the capabilities for Core Enterprise Services (CES), transport layers, metadata environments, enclaves, Communities of Interest (COIs), and federation that make Infrastructure Management possible.

3.1.3. Core Enterprise Services (CES)

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

CES will include but not be limited to storage management, messaging, transaction management, workflow management, search and discovery, directory services and service execution through an application server capability for control and management of multiple services, provide monitoring for Quality of Service (QoS), and governance of configuration and contract management to ensure a stable environment. The CES may also include emerging technologies such as Cloud Computing Services which includes; Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). These services may be obtain within the DoD Services Providers and the DoD Enterprise Cloud Service Broker.

- The contractor shall provide services and solutions that provide infrastructure capabilities to execute and manage content delivery services that deliver information to the warfighter and operational end user.
- The contractor shall ensure these solutions exploit the DoD CES when and wherever possible, and deliver AF-specific CES as required to augment the DoD CES to fulfill the AF mission.

3.1.4. Enclaves

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

An enclave is defined as virtual collections of hardware, software (including services), networks, and users that share common features, such as: authentication, authorization, trust, account directories, and policies.

- The contractor create services and solutions to identify a logical partitioning of the network and its information assets into capabilities-based enclaves, provide services and solutions to enable the establishment of trust relationships and inter-enclave credentialing through which enclaves can interoperate and control the direction and nature of information exchanges, allowing the execution of multi-enclave service threads.

3.1.5. Federation

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

- The contractor shall provide services and solutions that facilitate federation—a set of minimal agreements between enclave layer components which enable interaction between enclaves to take place transparently. Contractor services and solutions shall adhere to core specifications, standards, and technologies, such as PKI, SAML, JMS, and WS-* etc.
- The contractor shall provide federation capabilities within single domains and across multiple domains including domains within the DoD and IC to share mission critical information where applicable.
- The contractor shall establish naming and authentication between enclaves to enable discovery across them in accordance with applicable guidance, policy and direction.

3.1.6. Metadata Environments

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

Metadata environments include the generation, consumption, and management of metadata to enable the operational user to discover authoritative and aggregated data and support automated mediation where appropriate.

- The contractor shall provide services and solutions that help generate and manage metadata and Metadata Environments (MDEs) using COTS products when and where appropriate.
- Develop and sustain a metadata environment to be used in the discovery of information by end users and other services, the management of information assets for storage, retention, and records management, and security authorization and access control.
- The contractor shall develop MDEs in accordance with the DoD Enterprise Architecture Data Reference Model or IC Architecture Reference Model as appropriate and develop a federated query capability to enable end users to discover and exploit mission services to gain mission essential information.

- Metadata are characteristics or attributes of information assets, describing the type of information asset, its structure or syntax, and its content or semantics, plus a wide range of other attributes that assist users in finding, managing, and consuming information contained in assets.
- All metadata shall be created in accordance with the AF Metadata Specification and the DoD Discovery Metadata Specification (DDMS) or the IC Metadata specification as appropriate.
- Federated queries shall access MDEs within Enclaves to determine where information resides and how to access it. The MDE is characterized by the components and services it provides.

3.1.7. Metadata Components

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The MDE comprises the following components: Metadata Registry, Metadata Catalog and Service Registry.

3.1.8. Metadata Registry

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The metadata registry shall store COI vocabularies, and other metadata artifacts, describing the concepts and terminology required for information exchange within a COI. The vocabularies will be used by ADS's to format exposed information assets, and by the semantic discovery capability to allow users to find information assets and the services that deliver those assets.

- The contractor shall develop and support a Metadata Registry (MDR) to hold metadata definitions for the various types of metadata in a persistent store that is accessible during runtime operations.
- The contractor shall develop and support the capability for the MDR to track releasable information about individual artifacts and components of those artifacts where applicable.

3.1.9. Metadata Catalog

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The Metadata Catalogs will include metadata to describe individual information assets and that link those assets to the content delivery service that provides the asset to the end user.

- Asset delivered by the service should have content as an XML schema, PDF, or other Government approved format and adhering to the vocabulary prescribed by the COI that governs that information asset.

3.1.10. Service Registry

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The Service Registry shall track the identities and credentials of services within the enterprise information assurance infrastructure while supporting the invocation of services to deliver information assets once selected by an end user or another requesting service. Metadata Catalog entries shall point to services registered in the Service Registry, where the SOA infrastructure will be able to invoke the service to deliver the information asset to the requestor.

- The contractor shall leverage existing service registry and provide support for a Service Registry where all services are registered and stores information about implemented services, service interfaces, and the ports and bindings involved.

3.1.11. Metadata Environment Services

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

MDE services include the following: MDE Infrastructure Services, MDE Lifecycle Management, Discovery Services, and MDE Federation.

3.1.12. MDE Infrastructure Services

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

- The MDE infrastructure and solutions services shall provide and include, but are not limited to, information assurance, messaging, application hosting, storage management, and other core enterprise services.
- Create services that will also include or provide standard repository management services and solutions to support authorized administrative personnel in the creation, update, retrieval, and deletion of items within the MDE.
- The contractor shall provide infrastructure services to support MDEs.

3.1.13. Metadata Lifecycle Management

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

Metadata Lifecycle Management includes the following services: Metacards and Asset Registration, Automated Metadata Population Services (AMPS), Versioning and Indexing.

3.1.14. Metacards and Asset Registration

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

- The contractor shall provide services and solutions that support the manual or automatic population of metacards for registered assets in a structure that is compliant with DDMS or IC standards most current version and is in correlation with one or more COI vocabularies.
- The contractor shall provide services and solutions that support registering infrastructure services as assets, including, but not limited to, the following:

    1. Services developed to support COI business processes (e.g., content exposure, aggregation and presentation).
    2. Service interfaces based on one or more XML schemata, or other Government approved format.
    3. Vocabulary artifacts that describe COI domain knowledge. This includes, but is not limited to, Web Ontology Language (OWL) representations of knowledge, and XML Schema Definition (XSD) representations of message types.
    4. Information assets that are instances of authoritative content. This includes, but is not limited to, unstructured text documents, images, blob fields in databases and any other assets that qualify as requiring accountability of their content.

3.1.15. Automated Metadata Population Service (AMPS)

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

AMPS shall automatically create metacards for registration in the Metadata Catalog.

- User assets should be invoked to create metacards and be available as a service that can be called automatically during creation of an asset or in large scale metadata creation.

- The contractor shall develop and support an Automated Metadata Population Service (AMPS) to automatically create the metadata for an information asset or service.

3.1.16. Versioning

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The Contractor shall provide tools and services that will deliver version control of all metadata artifacts including but not limited to;

- Metacards, ontologies, and indexes; manage and control deprecation of artifacts such as COI vocabularies;
- Provide publication to consumers of versioning activities; ensure the application of the correct versions of the artifacts to other metadata services such as discovery, indexing, and automated metadata generation;
- Maintain histories and activity logs of metadata artifact versioning activities.

3.1.17. Indexing

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The Contractor shall provide tools and services that will deliver indexing capabilities to support discovery and management of information assets to include but not be limited to;

- Indexing of metacards using keywords, concepts, and other indexing schemes;
- The application of the ontologies generated from COI vocabularies to the indexing of artifacts;
- The generation of the indexes either from metadata artifacts such as XSDs and WSDLs or directly from information assets in other formats such as documents, emails, or presentations.

3.1.18. Semantic Discovery Services

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

- Semantic discovery users will be able to discover information based on their own preferred vocabulary, and automatically navigate across other users' vocabularies to find information relevant to each query.
- The semantic discovery capability will support both users seeking mission critical information as well as developers responsible for implementing new information capabilities for those users.
- The semantic discovery capability will pass DDMS metacard contents, rather than asset content, directly to consumers with delivery service invocation instructions which will be activated by consumers as required.
- The semantic discovery capability will federate with other DoD and IC Components and their information assets through the Joint DoD/DNI Federated Search Specification.

3.1.19. Federation of MDEs

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall provide services and solutions that support the federation of MDEs.

- Federation of MDEs will direct discovery queries to the right enclaves and, using the IA infrastructure, access information, and services across enclaves.

- The federation of MDEs will include the capability for MDEs to broadcast information requests and queries across all enclaves, if direct requests are not possible.

3.2. Enterprise Level Security (ELS)

3.2.1. Information Assurance Architecture

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall provide services and solutions to realize an information assurance architecture that permeates all components and operations. The contractor shall deliver information architecture services that conform to the Air Force Enterprise Architecture along with adherence to DoD and federal standards for information assurance, using role-based, policy-based or attribute-based controls, and managing trusted relationships between network enclaves. The contractor shall support the conformance with the 2-way authentication and end to end security stipulated by Implementation and Operation and the AF Information Assurance Enterprise Architecture. The contractor shall provide services and solutions in support of an information assurance architecture that delivers but is not limited to the following five categories of security services: confidentiality, integrity, availability, authenticity and non-repudiation. The contractor shall provide services and solutions to exploit the information assurance architecture to protect information consumed and generated by mission services. The contractor shall provide the capability of delivering these services at a level commensurate with the information assets being protected. The contractor shall provide infrastructure capabilities that enable SOA solutions to implement IA in accordance with WS assurance standards. WS standards will be defined however, the expected ones are:

WS-Security
WS-SecureConversation
WS-SecurityPolicy
WS-Trust
XML Signature
XML Encryption
XML Key Management (XKMS)

The contractor shall provide information assurance architecture, services, and solutions as stipulated by IC standards or other US, Allied, and Partner standards as specified in TO.

3.2.2. Confidentiality

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

- Provide confidentiality security services that prevent unauthorized disclosure of data, both while stored and during transit.

3.2.3. Integrity

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

- Provide integrity security services that prevent unauthorized modification of data, both while stored and in transit, and detection and notification of unauthorized modification of data.

3.2.4. Availability

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

- Provide availability services that ensure timely, reliable access to data and information services for authorized users.

3.2.5. Authenticity

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

- Ensure an authenticity service that applies to entities such as users, processes, systems, and information.

3.2.6. Non-Repudiation

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

- Provide non-repudiation services that ensure actions within the AF, DoD or IC SOA service invocations, information queries, etc., are attributable to the entity that invokes them.

3.2.7. Information Assurance Services

[Modify Information Assurance requirements as they relate to your Solicitation.]

Create services and solutions to implement and conduct IA operations such as, but not limited to, identity management, identity authentication, threat analyses and certification and accreditation.

The contractor shall ensure that all application deliverables meet the requirements of DoD Directive 8500.01E, Information Assurance, DoD Instruction 8500.2, Information Assurance Implementation, and DoD Instruction 8581.01, Information Assurance Policy for Space Systems Used by DoD, which supplements IA policy and requirements in the two aforementioned documents. Application deliverables should also meet Certification and Accreditation (C&A) requirements set forth in Intelligence Community Directive (ICD) 503, Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation, DoD Instruction 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP), and any other current standards and guidance that are applicable. Contractor solutions shall comply with the Federal Information Security Management Act (FISMA) and standards and guidelines set forth by the National Institute for Standards and Technologies (NIST) including Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, and its mandated reference SP 800-53, Security Controls for Federal Information Systems and Organizations, in addition to applicable Intelligence Community (IC) standards. The contractor shall support activities and meet the requirements of DoD Instruction 8520.02, Public Key Infrastructure (PKI) and Public Key (PK) Enabling, in order to achieve standardized, PKI-supported capabilities for biometrics, digital signatures, encryption, identification and authentication. These activities include but are not limited to defining user and registration requirements to Local Registration Authorities (LRAs).

For solutions to Infrastructure as a Service (IaaS), Platform as a Service (PaaS) or similar environments, and thus inherit existing network security controls, information security assurance is required at the Network layer of the TCP/IP DoD Model. The contractor shall ensure that all infrastructure deliverables comply with the Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) and Computer Network Defense (CND)., which includes the need for source code scanning, the DISA Database STIG, and a Web Penetration Test to mitigate vulnerabilities associated with SQL injections, cross-site scripting, and buffer overflows. The contractor shall also support activities and meet the requirements of DoDI 8520.02, Public Key Infrastructure (PKI) and Public Key (PK) Enabling, in order to achieve standardized, PKI-supported capabilities for biometrics, digital signatures, encryption, identification and authentication.

Personnel performing Information Assurance (IA) activities are required to obtain technical or management certifications to ensure compliance with DoD 8570.01-M, Information Assurance Workforce Improvement Program, 19 December 2005 (with all current changes), DoD Directive 8570.01, Information Assurance Workforce Training, Certification and Workforce Management, and as stipulated in Section H, Clause H101 of the overarching Network Operations (NetOps) and Infrastructure RFP.

3.2.8. Identity Management

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall provide services and solutions to accomplish identity management to enable users and applications to discover one another and utilize services provided by entities using methods such as the negotiated collaborative approach. The contractor shall also provide capabilities to selectively monitor interactions and manage all active identities to include user, services, machines, and services identity based on PKI.

The contractor shall provide services and solutions to accomplish life-cycle entity identity management from user creation to user revocation. Entities are defined as both human and non-human users possessing accounts within the enterprise. The contractor shall support user creation (identity confirmation, credentialing, enrollment), user management (provisioning across single or multiple systems and services, automated provisioning workflow, and self service), user access (identification, authentication, and authorization), and user revocation (de-provisioning and disablement). The contractor shall enable the de-provisioning process through automated account disablements and token revocation. The contractor shall provide access controls with rights, roles and privileges. The contractor shall provide the capability for all accounts to comply with Federal Information Protection Standard (FIPS) 196 or other specified standard in TO, by using approved methods of authentication such as, but not limited to, the following: Public Key Infrastructure (PKI) based authentication, One-Time Password Tokens, and Biometrics with PIN or password.

3.2.9. Threat Analysis

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

- Conduct comprehensive threat analyses for Network Defense of the SOA information assurance architecture in support of GIG Network Defense.

3.2.10. Certification and Accreditation

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

- The contractor shall provide services and solutions to help address the risks associated with AF network convergence into an interoperable enterprise and accomplish the certification and accreditation (C&A) of the AF SOA infrastructure and follow the DoD Information Assurance Certification and Accreditation Process (DIACAP) or ICD 503 to accomplish the infrastructure C&A as applicable.

- The contractor shall register the SOA infrastructure in the Enterprise Information Technology Data Repository (EITDR), and complete the Security, Interoperability, Supportability, Sustainability and Usability (SISSU) checklist, as described in the IT LEAN Reengineering and SISSU Guidebook, v5.0, 4 April 2007.

3.2.11. Enabling Security Capabilities

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall provide the following enabling capabilities to facilitate Warfighter access to critical mission capabilities:

1. Ensure all interactions between people, machines, and services are verified using security policy
2. Conduct confirmed 2-way authentication using DOD-PK I and Federal Bridge
3. Authorize access to data based on groups and roles credentials or applicable IC PKI and bridge
4. Monitor and log all activities to provide for both real time assessment and historical analysis
5. Use automated tools to analyze and detect anomalous behavior using real time/logged information to preclude and prevent internal attacks on Air Force information and computing resources
6. Delegate roles and groups based on policy
7. Mediate graduated access to data for various types of users
8. Enable efficient cross-domain information sharing across networks operating at different classification levels (e.g., SIPRNET, NIPRNET, and JWICS)
9. Operate, maintain, and configure point to point, VPN, and bulk encryption for network and longhaul circuits
10. Provide encryption to the base campus SIPRNet connectivity.
11. Provide SCI network security capabilities as specified in TOs.

3.2.12. Enterprise Service Management

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

- The contractor shall provide operation and maintenance of the SMI-ELS infrastructure including, but not limited to, network monitoring, load balancing, information archival and backup, disaster recovery, Continuity of Operations (COOP), and enterprise support desk (ESD). The ESD shall support users encountering issues in accessing mission capabilities.
- Provide lifecycle management of services for both requestors of services and service providers and establish processes to inform users of the availability of new version of services.
- The contractor shall provide enterprise service management to SCI networks as specified in TOs.

3.2.13. SMI-ELS Architecture Documentation

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

- The contractor shall document the Singularly Managed Infrastructure with Enterprise Level Security (SMI-ELS) within the AF Enterprise Architecture (EA).
- Document the Metadata Environment in the DoD EA Data Reference Model (DRM).
- Document the standards and protocols that the AF will enforce in the DoD EA Technical Reference Model (TRM).
- Develop DoD Architecture Framework (DoDAF) products or products adhering to other architecture guidelines as specified in Solicitations.
- Support process improvement events, such as AFSO21, to address SMI-ELS processes and issues. The contractor shall document AFSO21 products and engineered processes in the Process Reference Model (PRM) and DoD EA System Reference Model (SRM).

- Develop, document, and register SCI architectures and artifacts per TO directions and document engineering processes and process improvement activities and artifacts per TO directions for SCI systems and networks

3.3. Network Services and Solutions

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

- The contractor shall provide services and solutions that enable Network Operations and Network Infrastructure capabilities. Networks as defined in this section are for Data, Voice and Video.

3.3.1. Network Operations

[Modify Network Operations requirements as they relate to your Solicitation.]

The contractor shall provide services and solutions that enable Network Operations (NetOps) to operate and defend the Global Information Grid (GIG) to ensure information superiority such as land, air, and space networks across multiple levels of security.

- Provide capabilities that support the essential tasks, Situational Awareness (SA), and Command and Control (C2) that comprise the operational framework that comprise NetOps. The contractor shall support the following essential NetOps tasks: GIG Enterprise Management (GEM), GIG Network Defense (GND), and GIG Web Content Management.
- Provide services and solutions that help the Government attain the following desired effects in its management of the Global Information Grid (GIG):

  1. Assured System and Network Availability that ensures uninterrupted availability and protection of system and network resources. This includes providing for graceful degradation, self-healing, fail-over, diversity, and elimination of critical failure points.
  2. Assured Information Protection of information in storage, at rest, while it is passing over networks, including from the time it is stored and catalogued until it is distributed to users, operators, and decision makers.
  3. Assured Information Delivery of information to users, operators, and decision makers in a timely manner.

3.3.2. GIG Enterprise Management (GEM)

The contractor shall provide services and solutions that enable Enterprise Management to include traditional systems and network management (Fault Management, Configuration Management, Accounting Management, Performance Management, and Security Management), as well as information and infrastructure protection.

- Communicate elements and processes across a full spectrum of GIG information technology (IT) services to included but not limited to the following;

  1. Enterprise Services Management
  2. Systems Management
  3. Network Management
  4. Satellite Communications Management
  5. Electromagnetic Spectrum Management
  6. Cloud Computing Services

NOTE: Any current or planned acquisition of cloud services should be coordinated with the DISA DoD Enterprise Cloud Brokers Office and the Air Force Managed Services Office (MSO). Any use of third party, off-premises cloud services will require a waiver from the

GIG Waiver Panel IAW the Interim Guidance Memorandum on Use of Commercial Cloud Computing Services. Coordination will allow the DoD Enterprise Cloud Service Broker Office and the AF MSO to appropriately assess risk of all cloud services and allow the Information Assurance (IA) team to provide more information based on the specifics of the planned implementation.

❖ **Points of Contact (POC)**

Air Force Managed Services Office (MSO)
Mr. Michael Clark
Commoditized Infrastructure Branch Chief
DSN: 845-6840
Comm: 781-225-6840
Michael.Clark@Hanscom.AF.Mil

Air Force Managed Services Office (MSO)
Julie Mintz
Cross Functional Solutions
Defense Information Systems Agency
DSN: 375-5753
Comm: 301-225-5753
julie.j.mintz.civ@mail.mil
julie.j.mintz.civ@mail.smil.mil

3.3.3. Enterprise Messaging and Directory Services

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall provide services and solutions that enable directory services, e-mail and organizational messaging in accordance with Enterprise Architecture.

3.3.4. Enterprise Application Services and Service Management

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall provide services and solutions that enable service management and the management of enterprise application services, including, but not limited to, the following:

1. Monitoring and measuring application and service health and performance
2. Reporting and visualizing key application and service QoS metrics
3. Monitoring and enforcing service level agreement (SLA) compliance
4. Managing application and service lifecycles
5. Provisioning applications and services
6. Platform as a Service (PaaS)
7. Software as a Service (SaaS)
8. Infrastructure as a Service (IaaS)
9. Logging and auditing application and service activities
10. Anticipating application and service problems and sending alert notifications
11. Pinpointing the root cause of application or service problems and allocating resources to correct the problems
12. Automating failover and load balancing

13. Mediation services transforming service messages and performing content based routing
14. Correlating enterprise service messages for business transaction tracking

3.3.5. Enterprise Information Management

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall provide services and solutions that enable information management services, including, but not limited to, the following:

1. Collaboration Services
2. Continuity of Operations
3. Disaster Recovery
4. Data Storage
5. Storage Area Network
6. Network Attached Storage
7. Infrastructure as a Service (Iaas)
8. Platform as a Service (PaaS)
9. Software as a Service (SaaS)
10. Back-Up/Archive
11. Records Management

3.3.6. GIG Network Defense (GND)

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall provide services and solutions that enable GIG Network Defense, including, but not limited to, the following:

Information Assurance (IA) – Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This shall include, but not be limited to, providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. IA services shall include, but not be limited to:

a. Assured Information Sharing and Management
b. Access Control
c. Cross-Domain Security
d. Information Environment Protection
e. Certification and Accreditation
f. Risk Analysis
g. IA Awareness
h. Auditing
i. Emanations Security (EMSEC) /TEMPEST for TS or SCI environments
j. Communication Security (COMSEC)
k. Operation Security (OPSEC)
l. Information Protection
m. Authentication
n. Resource Protection
o. Federated Identity Management
p. Virtual Private Networking
q. Network Protection
r. Filtering
s. Intrusion Detection and Prevention
t. Cryptographic Services

u. Key and Certificate Services
v. Insider Threat Protection
w. Anomalous behavior detection
x. Time Compliance Network Order (TCNO)
y. Computer Incident Response Team (CIRT)
z. Air Force Computer Emergency Response Team (AFCERT)
aa. Telecommunications Monitoring and Assessment Program (TMAP)

1. Computer Network Defense (CND) – Defensive measures to protect, monitor, analyze, detect, and respond to unauthorized activity with DoD information systems and computer networks and defend information, computer, and networks from disruption, denial, degradation, or destruction. This shall include, but not be limited to, the employment of IA capabilities in response to CND alert or threat information and the capability to predict, analysis and defend against new attack vectors.
2. Computer Network Defense Response Actions (CND RA) – Deliberate, authorized defensive measures or activities that protect and defend DoD computer systems and networks under attack or targeted for attack by adversary computer systems/networks. The contractor shall also rapidly and accurately implement JTF-GNO and NetOps directed Information Operations Condition (INFOCON) changes and provide Command and control on the progress and completion.
3. Defense Critical Infrastructure Protection (CIP) – Actions taken to prevent, remediate, or mitigate the risks resulting from critical infrastructure vulnerabilities. Actions shall include, but not be limited to, changes in tactics, techniques, or procedures; adding redundancy; selection of another asset; isolation or hardening; guarding; etc.

3.3.7. GIG Web Content Management

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall provide services and solutions to develop and administer web sites that enable Web Content Management and help ensure information is available to users on the GIG to accomplish their mission. Capabilities shall include, but not be limited to, those that enable the following core services areas:

1. Web Content Discovery – The ability to quickly search for information throughout the GIG. The contractor shall provide the capability for operational staffs to search across multiple sources from one place using a web crawler and web browser, vice making several attempts. Once products are located, the Content Delivery service shall permit users to pull in needed products.
2. Web Content Delivery – Delivery of requested information to GIG users. The contractor shall provide the capability for timely delivery of items across multiple, heterogeneous communication systems with delivery and read receipt notifications, providing assured delivery of information products.
3. Content Storage – The contractor shall provide and support physical and virtual places to host data on the network throughout the GIG with varying degrees of persistence.

- The contractor shall provide services and solutions that provide Network Operations Centers with capabilities such as, but not limited to, the following:

1. The ability to optimize the flow and location of information over the GIG by positioning and repositioning data and services to optimum locations on the GIG in relation to the information producers, information consumers, and the mission requirements.
2. The ability to ensure that the GIG is optimally delivering the information required by GIG users in accordance with information delivery priorities.
3. The visibility of information flowing across the GIG and of those systems used to store, catalog, discover, and transport information.

4. Tools to view information flows and access, determine impact to network capacity, and ensure user profiles are being satisfied with a reasonable quality of service.
5. The capability to prioritize information requirements, determine the sources responsible for providing that information, and stage information content throughout the GIG in support of a given operation.

6. The ability to track and maintain knowledge of various requests and user profiles for information.
7. The ability to coordinate changes in operating parameters of GIG assets.
8. The ability to review and validate the user-profile database.

3.3.8. Network Operations Enabling Capabilities

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall provide services and solutions that accomplish or provide the following enabling capabilities:

1. Distributed Network Connectivity – Robust, redundant data paths and nodes with both physical and logical diversity to maximize effectiveness and eliminate single points of failure.
2. Continuity of Operations (COOP) – Plans and capabilities to enable uninterrupted NetOps operations with seamless transfer of operations, especially network C2 following outages at any key NetOps sites. These shall include, but not be limited to, fully redundant backup capabilities with automatic failover that is transparent to users.
3. Information Management and Exchange – Automated tools and processes to facilitate the exchange of information and to aid operators in visualizing network operations and events, to facilitate rapid event characterization and information exchange, and to keep pace with rapidly changing networks. Operate the Base Information Transfer System and Official Mail Center. Provide Privacy ACT, Freedom of Information Act (FOIA), and record management training.
4. Standardization – Standardization of configurations, processes, and applications across the enterprise from the gateways to the desktops to facilitate centralized management, enhance security through configuration control, and save manpower in certification and accreditation, patch implementation, hardware/software upgrades, and asset tracking.
5. Risk Management – A multi-faceted and global approach for risk management on applications currently residing on the network and new applications waiting to be fielded. This approach shall assess the benefits of adding the application to the network and any security risks it may introduce, the ability to execute corrective actions or configuration control measures, and the potential effect any change would have on network configuration, services, or other applications. This process shall apply across MAJCOMs and include arbitration processes in the event of a conflict between the intended user and others. Solutions shall follow Government approved standards such as the Information Technology Infrastructure Library (ITIL) framework.
6. Change Management – Tools, tactics, techniques and procedures for accomplishing change management across the AF enterprise to help implement network operational concepts.
7. Training – Resources need to provide training such as training materials, instructors and facility.
8. System Administrator- Set up, configure, develop, maintain, troubleshoot, and support internal and external networks
9. Database Management- Perform loads, upgrade, patches, data recovery, backups and maintain active directory.

10. Account Management – Creation, delete, and modify voice, data, and video accounts and provides means to unlock Common Access Card (CAC)

3.3.9. Network Command and Control (C2)

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall provide services and solutions that enable network command and control, including, but not limited to, the following:

- The consolidation of network situational awareness (SA) services and solutions that integrate command and control (C2) capabilities, eliminate the need for scheduled manual reporting, and provide the warfighter with on-demand, real-time operational status of networks, core services, and applications directly serving or influencing his or her Area of Responsibility.

1. Rapid characterization and response to anomalous activity, including, but not limited to, “low and slow” network probe and exploitation efforts, and implement appropriate defensive actions or countermeasures.
2. Trend analysis and correlation of network incidents (e.g., probes, intrusions, and virus outbreaks), outages, and degradation events.
3. Rapid implementation of security countermeasures by facilitating the coordination of network restoration priorities and actions after an intrusion or adverse network event.
4. Coordination and reallocation of limited resources (e.g., bandwidth, frequencies) in response to multiple and/or conflicting warfighter requirements.

3.3.10. Network Management and Enterprise Services

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall provide services and solutions that accomplish Network Management for AF Network Operation Center (AFNOC)/ Integrated Network Operations and Security Center (I-NOSC) activities such as, but not limited to, the following:

1. Automation and enforcement of network policy
2. Operation of network sensors
3. Monitoring and analysis of network behavior
4. Network performance analysis and tuning
5. Network counter measures.
6. Network boundary management and control.
7. Network security access
8. Network service orchestration
9. Execution of INFOCON
10. Asset management to include Equipment Management

- The contractor shall provide services and solutions that accomplish Network Management and Support for the Enterprise Support Unit (ESU) and the Enterprise Service Desk (ESD) anticipated activities such as, but not limited to, the following:

1. Network configuration management
2. Load balancing
3. Vulnerability analysis and response
4. Application and content management
5. Continuity of Operations (COOP) management
6. Resource virtualization
7. Information lifecycle management
8. Service Orchestration

9. Virtualized IT service support
10. Help Desk/Call Center
11. Security Management Service

- The contractor shall provide services and solutions that accomplish Enterprise Services to support Network Operations such as, but not limited to, the following:

1. Information technology (IT) service virtualization
2. IT Support
3. Service/security management and provisioning
4. Domain security
5. Cross-domain security
6. Collaboration (video teleconference)
7. Content and service staging
8. Federated content discovery
9. Application, system, services and data hosting
10. Development of applications for database or web pages
11. Producer to consumer availability of service
12. Configuration and change management
13. Platform as a Service (PaaS)
14. Infrastructure as a Service (IaaS)
15. Software as a Service (SaaS)

TOs from other agencies, departments, or AF functional communities for the same purpose may be issued. These TOs may specify and substitute other standards, guidance, and applicable within their TO to provide solutions tailored to meet their network management and enterprise services strategies.

3.3.11. Network Infrastructure

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall provide services and solutions in support of transport layer capabilities to deliver the physical infrastructure upon which the SOA middleware and services operate, including, but not limited to, messaging capabilities and site preparation and installation services. Support of the transport layer includes the AF's Information Transport System (ITS) which is the engineering, installation, and sustainment of the high-performance, survivable fiber optic backbone to include "wired" and "wireless" networks.

3.3.12. Messaging

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

- The contractor shall provide messaging capabilities allowing separate, uncoupled applications to reliably communicate asynchronously.
- The contractor shall provide delivery pathways, such as Web services, HyperText Transfer Protocol (HTTP) or HyperText Transfer Protocol Secure (HTTPS) connections, or other links, as needed to support content delivery and presentation service requests.
- The contractor shall tag and register delivery pathways as necessary.
- The contractor shall support other data transport pathways, such as File Transfer Protocol (FTP) and Open DataBase Connectivity (ODBC), for legacy systems and databases.

Include the following, but not limited to, the design and/or implementation of:

- messaging architecture;
- point-to-point distribution of messages;

- publish-subscribe distribution of messages;
- message producer;
- message consumer;
- one-way interaction between a message producer and a message provider;
- request-reply interaction between a message producer and a message consumer;
- connectivity between an application and a messaging provider.

Provide messaging services that encompass, but are not limited to, provision of federated, distributed, and fault-tolerant enterprise messaging capabilities;

- message publishing and subscribing, peer-to-peer messaging and queuing;
- support for the configuration of QoS parameters for a published message, including the priority, precedence, and time-to-live (TTL);
- provision of guaranteed delivery to disconnected users or applications;
- development of Online Asynchronous Processing (OLAP) and real or near real-time enterprise data reporting capabilities.

3.3.13. Site Preparation and Installation Services

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall perform site preparation and installation activities to support implementation of required services and solutions under this contract at any AF, DoD, or other Federal Agency location.

3.3.14. Requirements Analysis and Conceptual Design

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall perform requirements analyses and conceptual designs at required locations. During this process, the contractor shall collect all the information to complete a requirements analysis and conceptual design. The contractor shall survey, evaluate, and provide technical advice concerning all existing infrastructures, communications, power, Heating, Ventilation and Air Conditioning (HVAC), and environmental aspects of the site. The contractor shall provide an implementation plan, in accordance with the Solicitation, reflecting the strategy, schedule, and recommendations (e.g., site architecture, topology, and configuration) for the implementation with considerations of on-site failover and continuity of operations. The Government will provide applicable information, as available, such as existing/projected user network resources and locations, GFE, base support requirements, and other written information related to specific implementation for each Solicitation to establish the unique characteristics of each site. Access to Government facilities will be provided and interviews shall be coordinated with Government points of contact specified in the Solicitation.

Types of support and services provided by the contractor shall include, but not be limited to: Email, Server and Storage Area Network Administration, Security Boundary Administration, Print Management, Configuration/Release Management (i.e. Security/Patch Administration, etc), Mobile/Remote User Services Support and Administration, Network Infrastructure Management and Administration, Certification and Accreditation (i.e. Security Scanning, etc), Directory Services, and Event Management.

The contractor shall possess reach back capabilities to obtain expertise that may not be immediately available onsite and the ability to surge in times of crisis.

The contractor is required to deliver all services and solutions provided under this contract described below. The contractor shall design, develop, install, document and test custom solutions and their infrastructures. The contractor shall enable system solutions to integrate with: Air Traffic Control, Land Mobile Radio, Command Post Switches, Defense Red Switch (DSR), Defense Red Switch Network (DRSN), Giant Voice, Enhanced 911, Cell Systems, Base Altering Systems and Crash Nets, and any other systems specifically identified in the Solicitation.

3.3.15. Site Survey

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall perform site surveys at required locations. The findings of the site survey and any actions required in preparation for system installation shall be documented.

3.3.16. Systems Engineering

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

[NOTE: If applicable, insert additional MAJCOM or organization Systems Engineering Process (SEP) policy, requirements or guidelines. Include any special SEP instructions for Top Secret/TS SCI systems or applications.]

The contractor shall provide systems engineering solutions for the analysis, design, integration, installation, testing, and life-cycle support of new and upgraded systems associated with delivery of infrastructure capabilities as defined by the AF enterprise architecture. The contractor shall employ disciplined systems engineering processes in accomplishing contract taskings, using commercial best practices in accordance with of AFI 63-1201, Life Cycle Systems Engineering, for systems engineering processes in planning, architecting, requirements development and management, design, technical management and control, technical reviews, technical measurements, integrated risk management, configuration management, data management, interface management, decision analysis, systems management, inspections and maintenance, sources of supply maintenance and repair, and test and evaluation, verification and validation. These systems engineering solutions shall follow industry standard engineering processes and may include but not be limited to: Technical assessments of all user requirements, integration of all GFE and Contractor Furnished Equipment (CFE) as proposed, hardware and software information, network applications, system design, training (COTS or customized)(initial and recurring), maintenance and support, system interface studies and control documents, network integration and test plans, cost analysis/trade-off studies, engineering change proposals, Voice Switching System (VSS) facility and systems/applications studies, VSS call detail recording and traffic measurement data analysis, engineering support (digital transmission/switching equipment) to Government engineers. The contractor shall provide reengineering capabilities to examine structures, systems and roles for the purpose of executing a ground-up redesign for achieving long-term, full-scale integration required for the GIG.

Solicitations will further refine the systems engineering processes according to MAJCOM or functional policies and practices. The contractor shall employ the principles of open technology development described in the DoD Open Technology Development Guidebook and in Net-Centric Enterprise Solutions for Interoperability (NESI) body of knowledge, and systems engineering activities used in developing contractor solutions shall adhere to open architecture designs for hardware and software, and employ a modular open systems architecture approach. The contractor's systems engineering planning and design activities shall also adhere to the DoD's Information Sharing and Net Centric Strategies published by the DoD CIO and the engineering body of knowledge and lesson's- learned accumulated in NESI. TOs may require adherence to other governmental standards.

3.3.17. System Upgrade/Update Support

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall provide system upgrade support and future planning associated with delivery of infrastructure capabilities as defined by the AF enterprise architecture.

- Maintain current design and develop systems similar to those implemented in the VSS and update the Government of changes and strategies.
- Identify current problems or anticipate areas relating to telephony hardware and software systems and present the Government with technical issues of interest or value regarding VSS
- Provide information regarding new emerging technology advancement to the Government and support new telecommunication products that are approved by the DoD JITC and introduce into the VSS network and must adhere to AF or IC security requirements.

3.3.18. Post-Cutover Support

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

Each solution shall include a warranty as specified in Section I, Clause 52.246-17. In addition to FAR Clause 52.246-17, the following additional requirements apply: Users shall have highly reliable and maintainable telephony products and system solutions to interoperate with the described environment. Components shall be maintainable and expandable by the user without voiding the warranty coverage.

In addition to any OEM warranty coverage, three types of post cutover operation and maintenance support shall be provided: System Support, Workmanship Support, and Construction Support. The contractor shall provide for restoration of the system and repair of equipment in a timeframe specified as required by this contract, unless stated otherwise in the Solicitation. The means to transport equipment and repair personnel both to and from the Government site is the responsibility of the contractor. The contractor shall provide technical support, software support, and hardware replacement for failed components, engineering support, and maintenance services necessary to ensure active management, reliable operations, and rapid restoration. These technical support services shall include Tier II to Original Equipment Manufacturer (OEM) level support as required based on the need to achieve problem resolution. All technical support shall be provided by certified technical personnel fluent in the English language. If the Offeror is alerted to a degradation or failure, the Offeror shall provide immediate support to the operational user to identify, troubleshoot, and remedy the problem. The Offeror shall execute all hardware repair actions necessary to return the affected system to full operational capability. If the failed equipment is no longer under any alternative warranty support, the Offeror shall provide replacement equipment. Technical support shall be provided on a continuous, as-needed basis twenty-four (24) hours per day, 365 days per year for systems, peripherals, applications, and devices deployed. The contractor shall provide toll free, email, DSN, and PSTN access capabilities to contact requesting support for support issues.

3.3.19. Design/Integration Reviews

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall conduct design and integration reviews if required in the Solicitation and in compliance with disciplined system engineer processes. This may be a formal or informal preliminary and final design reviews.

The contractor shall provide a single source of integration management for worldwide support, planning and sustainment of dissimilar manufacturer's switching systems, applications and peripheral equipment related to the VSS. The contractor shall identify cross functional applications and technical issues from selected symbiotic functional areas and document the opportunities for resolving the issues. The contractor shall report impacts on the issues such as costs, return on investment, schedule dependencies and recommend functional and technical solutions. The contractor shall identify integration issues and problems such as requirements definition, architecture and policy/standards compliance and engineering guidelines compliance. The contractor shall enable convergence with data systems and/or collaborative tools as specified and required in the Solicitation.

3.3.20. Prototypes

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall develop schedules and implementation plans with definable deliverables, including parallel operations where required, identification of technical approaches, and a description of anticipated prototype results associated with delivery of infrastructure capabilities as defined by the AF DoD or applicable IC enterprise architecture.. The contractor shall operate and maintain prototype applications, infrastructures, models and databases to determine optimal solutions for integration concepts and problems integral to the integration process.

3.3.21. Preliminary Design/Integration Review (PDR)

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

During the PDR, the contractor shall present initial draft system design associated with delivery of infrastructure capabilities as defined by the enterprise architecture. for Government review.

The draft documents to be reviewed shall include those specified in the Solicitation. Examples may include the system requirements, the final Site Survey Report, System Design, Installation Specification (IS), Engineering Drawings and Installation Plan. This review shall include a list of recommended long-lead time items that the Government must order and have available at the time of system installation. This review shall be in sufficient detail to ensure technical understanding of the following: mission and requirements analysis, identification of all equipment and software to be integrated and to be used in the development of the design, and the scope and schedule of the work to be performed.

3.3.22. Final Design/Integration Review (FDR)

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

During the FDR, the Contractor shall present final system design documentation associated with delivery of infrastructure capabilities as defined by the enterprise architecture.for Government review. The documents shall consist of those identified in the Solicitation. Upon Government approval of the FDR documentation, the Contractor will be authorized to proceed with the installation. If discrepancies are identified, the Contractor shall correct all discrepancies and another FDR may be required at the discretion of the Government.

3.3.23. Site Preparation

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

As part of an overall system design and installation, the contractor may be required to perform site preparation support as required by the IS and approved by the Government Contracting

Officer. The Government may, at its option, perform any portion or all of the requirements documented in the site survey report. Base civil engineering functions (or equivalent) will be used whenever possible. The contractor shall work with the base Contracting Officer's Representative (COR) to accept civil engineering functions (or equivalent) as being in accordance with the approved implementation plan prior to beginning work. The final IS shall specify what site preparation the Government will perform and what site preparations the contractor will perform.

3.3.24. Pre-Installation Briefing

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

As required by the Solicitation, the contractor shall present pre-installation briefings at the user sites. These briefings shall include the implementation strategy, installation schedule, verification that all allied support is completed and the site is ready for installation, and discussions of any potential problem areas. Additional pre-installation briefings may be held, as required by the Government.

3.3.25. Government Support

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The Government will furnish facilities and utilities to the Contractor, including light, heat, ventilation, electric current, and outlets for use by installation personnel as required and stated in Solicitations. These facilities and utilities will be provided as specified in the Site Survey Report. These facilities will be readied prior to arrival of Contractor personnel and be provided at no cost to the Contractor. The Contractor shall provide required temporary utilities, which are not readily available in the work area. The Contractor shall coordinate, through the on-site COR, any requirement before temporary disconnection of a utility. The Contractor shall submit a request in writing to the on-site COR fourteen (14) days in advance of the necessity of utility disconnection.

3.3.26. Installation

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall engineer, install, configure, modify, relocate, or remove Communication and Information (C&I) systems for operational use. The systems and equipment installations or modifications must comply with established architectures. The contractor shall perform validation and verification testing on the system, assist users in configuring the system to meet their system requirements, and provide all applicable operating manuals/system management guides. Further, the contractor shall provide pre-cutover and post-cutover on-site training IAW with Solicitations. The government will identify personnel who will receive this training. The training shall provide for in-depth hands-on maintenance, operations and database administration.

3.3.27. Inside Plant

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall, (as required by each Solicitation), install and configure of all the components for inside plant (e.g., power, groundings, HVAC, racks, fiber optic distribution panels, equipment, internal cabling, comm. closet, etc). The contractor shall install and test all cable and components IAW accepted industry standards, unless superseded by a Government approved IS indicated within the Solicitation. Electrical and communications cable, conduits, and circuits shall be installed IAW the National Electric Code (NEC). The contractor shall clearly label each end of every individual cable in accordance with the floor plans or engineering drawings. The contractor shall provide attached labels that are durable and legible. For any deviations to the specific installation specification, the contractor shall submit a proposal to the contracting officer for approval.

3.3.28. Outside Plant

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall, as required by each Solicitation, install and configure of all the components for outside plant (e.g., fiber, manholes, duct, building entries, trenching, digging, constructions, external cabling, etc). The contractor shall install and test all cable and components IAW accepted industry standards, unless superseded by a Government approved IS indicated within the Solicitation. Electrical and communications cable, conduits, and circuits shall be installed IAW the National Electric Code (NEC). The contractor shall clearly label each end of every individual cable in accordance with the floor plans or engineering drawings. The contractor shall provide attached labels that are durable and legible. For any deviations to the specific installation specification, the contractor shall submit a proposal to the contracting officer for approval. The contractor's design should not include aerial cable unless the Government has approved specific site exceptions. When use of aerial cable is approved, installation and test shall be IAW accepted industry standards, unless superseded by a Government approved IS indicated within the Solicitation.

3.3.29. Tools and Testing Support

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall provide all tools, installation materials, and test equipment required to perform any required product installation and maintenance as called for by the Solicitation. All tools and test equipment shall remain the property of the contractor. Any damage caused by the contractor to existing site facilities or equipment which might occur during site preparation, installation, testing or cutover of the system will be repaired at the expense of the contractor unless otherwise directed by the Government. The site shall be restored to the original condition which existed prior to the event unless otherwise directed. The Solicitation will specify testing and inspection requirements. The contractor shall demonstrate that the system design meets the reliability / availability / maintainability requirements of the Solicitation. Mean Time Between Failure data will be used to calculate the reliability / availability / maintainability of the system. The calculations shall be based on all of the equipment installed in the network. The contractor shall be capable of performing reliability, availability, and maintainability analyses of components, isolated sub-networks and the entire system.

3.4. Dynamic Test Environment

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall provide tools and services to support the design, implementation, and operation of a dynamic test environment. The dynamic test environment will enable applications developers to deploy their applications and services into the infrastructure and test the operation of those applications and the effect of those applications on other fielded capabilities.

3.4.1. Design

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall provide tools and services to support the design of the dynamic test environment. This will include but not be limited to defining concepts for dynamic testing;

Articulating processes and procedures for conducting dynamic testing; architecting the test environment; evaluating and selecting products and technologies for the test environment.

3.4.2. Implementation

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall provide tools and services to implement the dynamic test environment. This will include but not limited to configuring the products and technologies required by the design of the test environment; installing those products and technologies in location designated by the design; developing capabilities necessary to fully integrate the products and technologies with each other and with existing infrastructure capabilities; integrating the products, technologies and developed capabilities with existing infrastructure capabilities to configure the test environment; and developing and executing test procedures to ensure the proper functioning of the test environment.

3.4.3. Operation

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall provide tools and services to operate the dynamic test environment. This shall include but not be limited to developing operating procedures, user guides, training materials, and other documentation to ensure to correct use of the test environment by users; developing administrative and management processes and documentation to ensure proper operation of the test environment in support of end users; monitoring the operation of the test environment to ensure users are achieving their test objectives; conducting performance evaluations of the test environment; and scheduling and executing technology refreshes and other activities to ensure the ongoing operation of the test environment.

3.5. Communication Operations and Maintenance (O&M)

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall provide services and solutions that accomplish O&M that include, but not limited to the following:

1. Operations and Telephony Infrastructure to include telephone customer support
2. Meteorological and Navigational Aids (METNAV)
3. Land Mobile Radios (LMR)
4. Personal Wireless Communication Systems (PWCS)
5. Video Teleconferencing (VTC)
6. Satellite Communications (SATCOM)
7. Air Traffic Control and Landing Systems (ATCALS)
8. Radar
9. Computer Systems Control (Tech Control) including but not limited to Circuit Management, Circuit Management Office, and Telecommunications Manager
10. Electronic Communication Management
11. Visual Imagery
12. Multimedia Services
13. Intrusion Detection
14. Deployment Manager
15. Antennas

3.6. General Requirements

[The General Information Section is here to capture all the requirements that do not logically fit or are not specifically covered in any of the other sections. Modify as needed to meet your requirement. This section may include such things as required quality control plans or systems, location of the work, hours of work, physical security, emergency or special events, environmental or hazardous requirements, security requirements, specific training

requirements, Modify each section IAW your requirements.] Sections 3.6-3.6.32 are example requirements that will help you facilitate the development of your PWS. [Delete those that do not apply.]

3.6.1. Enterprise Software Initiative

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

In situations where the purchase of new COTS software is needed to satisfy the requirements of a particular Solicitation, the contractor shall first use available existing enterprise licenses, then products obtained via the DoD's Enterprise Software Initiative (ESI) Blanket Purchase Agreements (BPAs). The updated listing of COTS software available from DoD ESI sources can be viewed on the web at http://www.esi.mil.

3.6.2. Hardware

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

All hardware provided in support of solutions under this contract shall include all software and associated hardware required for operations (such as controllers, connectors, cables, drivers, adapters, etc.) as provided by the OEM.

3.6.3. Software Support

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

Unless specified otherwise in the Solicitation, the contractor shall fully support all unique software developed to support integrated solutions on this contract. The contractor shall support all software revisions deployed or resident on the system, and sub-systems. The data rights ownership/licensing guidance is specified in DFARS 252.227-7013(b) and (e) and DFARS 252.227-7014(b) and (e) and DFARS 252.227-7017. The Contractor shall disclose to the ordering Contracting Officer and ordering office in any proposal for a Solicitation, or after award of a Solicitation if not previously disclosed in the proposal, any technical data or non-commercial computer software and computer software/source code documentation developed exclusively at government expense in performance of the Solicitation.

3.6.3.1. Data Rights and Non-Commercial Computer Software

In order to implement the provisions at DFARS 252.227-7013(b) and (e) and DFARS 252.227-7014(b) and (e) and DFARS 252.227-7017, the Contractor shall disclose to the ordering Contracting Officer and ordering office in any proposal for a Solicitation, or after award of a Solicitation if not previously disclosed in the proposal, any technical data or non-commercial computer software and computer software/source code documentation developed exclusively at government expense in performance of the Solicitation. This disclosure shall be made whether or not an express requirement for the disclosure is included or not included in the PWS or solicitation for the order. The disclosure shall indicate the rights asserted in the technical data and non-commercial computer software by the Contractor and rights that would be acquired by the government if the data or non-commercial software was required to be delivered under the Solicitation and its CDRL requirements and any cost/price associated with delivery. This disclosure requirement also applies to segregable routines of non-commercial software that may be developed exclusively at Government expense to integrate Commercial Software components or applications provided under a commercial software license or developed to enable Commercial Software to meet requirements of this Solicitation. Performance of this disclosure requirement shall be considered a material performance requirement of any Solicitation under which such technical data or non-commercial computer software is developed exclusively at Government expense.

3.6.4. Government Furnished Equipment

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

Under some Solicitations, the Government will provide products acquired under this contract, other contracts, and GFE identified in site specific Solicitations. The contractor's design shall incorporate existing systems/subsystems to the maximum extent possible, based on cost/technical tradeoff analysis conducted during the engineering process to ensure security and resource sharing of both Government Furnished Equipment (GFE) and Contractor Furnished Equipment (CFE).

3.6.5. Government Furnished Property

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

[Identify any GFE and/or GFI, and any limitations that will be provided to the contractor. For GFE, provide serial numbers and all identifying information. (Note: If GFE is a sizable list, indicate for example, "50 PC Pentium IVs," and state that serial numbers will be provided at contract/TO award, along with location and delivery method.) For GFI, list by document number and title, date, etc. Include standards, specifications, and other reference material required to perform the contract/TO. Include any facilities the Government may need to provide to contractor personnel for project performance.]

When the contract requires the contractor to work in a Government facility, the Government will furnish or make available working space, network access, and equipment to include:

- Windows PC with Microsoft Office Suite (Outlook, Word, Excel, PowerPoint, etc.)
- Telephone (local and long distance calls authorized as dictated by contract performance requirements)
- Facsimile
- Copier
- Printer

Copies of required Government furnished materials cited in the solicitation, PWS, DD Form 254, and/or in the contract will be provided to the contractor in hard copy or soft copy. All materials will remain the property of the Government and will be returned to the cognizant Government COR upon request or at the end of the contract period of performance.

Equipment purchased by the contractor with the approval of the Government and directly charged to this contract shall be considered government owned-contractor operated equipment. The contractor shall conduct a joint inventory and turn in this equipment to the COR upon request or completion of the contract.

3.6.6. Billable Hours

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

In order for man-hours to be billed, deliverable services must have been performed in direct support of a requirement in the TO PWS. In the course of business, situations may arise where Government facilities may not be available for performance of the TO requirements (i.e., base closure due to weather, Force Protection conditions, etc.). When the base is officially closed no contractor services will be provided and no charges will be incurred and/or billed to any TO. There may also be occasions when support contractors are invited to participate in morale and recreational activities (i.e., holiday parties, golf outings, sports days and other various social events). Contractor employees shall not be directed to attend such events by the Government. Since a contract employee is not a government employee, the contract employee cannot be granted the same duty time activities as Government employees. Participation in such events is not billable to the TO and contractor employee participation should be IAW the employees, company's policies and compensation system.

3.6.7. Non-Personal Services

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The Government will neither supervise contractor employees nor control the method by which the contractor performs the required tasks. Under no circumstances shall the Government assign tasks to, or prepare work schedules for, individual contractor employees. It shall be the responsibility of the contractor to manage its employees and to guard against any actions that are of the nature of personal services, or give the perception of personal services. If the contractor feels that any actions constitute, or are perceived to constitute personal services, it shall be the contractor's responsibility to notify the Solicitation (TO) Contracting Officers CO immediately. These services shall not be used to perform work of a policy/decision making or management nature, i.e., inherently Governmental functions. All decisions relative to programs supported by the contractor shall be the sole responsibility of the Government. These operating procedures may be superseded by Theater Commander's direction during deployments.

3.6.8. Contractor Identification

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

All contractor/subcontractor personnel shall be required to wear AF-approved or provided picture identification badges so as to distinguish themselves from Government employees. When conversing with Government personnel during business meetings, over the telephone or via electronic mail, contractor/subcontractor personnel shall identify themselves as such to avoid situations arising where sensitive topics might be better discussed solely between Government employees. Contractors/subcontractors shall identify themselves on any attendance sheet or any coordination documents they may review. Electronic mail signature blocks shall identify their company affiliation. Where practicable, contractor/subcontractors occupying collocated space with their Government program customer should identify their work space area with their name and company affiliation. Reference Clause H063 of the basic ID/IQ contract.

3.6.9. Training

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

Contractor personnel are required to possess the skills necessary to support their company's minimum requirements of the labor category under which they are performing. Training necessary to meet minimum requirements will not be paid for by the Government or charged to TOs by contractors.

3.6.9.1. Mission-Unique Training

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

In situations where the Government organization being supported requires some unique level of support because of program/mission-unique needs, then the contractor may directly charge the TO on a cost reimbursable basis. Unique training required for successful support must be specifically authorized by the TO CO. Labor expenses and travel related expenses may be allowed to be billed on a cost reimbursement basis. Tuition/Registration/Book fees (costs) may also be recoverable on a cost reimbursable basis if specifically authorized by the TO CO. The agency requiring the unique support must document the TO file with a signed memorandum that such contemplated labor, travel, and costs to be reimbursed by the Government are mission essential and in direct support of unique or special requirements to support the billing of such costs against the TO.

3.6.9.2. Other Government-Provided Training

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor's employees may participate in other Government provided training, on a non-discriminatory basis as among contractors, under the following circumstances:

a) The contractor employees' participation is on a space-available basis,
b) The contractor employees' participation does not negatively impact performance of this Solicitation,
c) The Government incurs no additional cost in providing the training due to the contractor employees' participation, and
d) Man-hours spent due to the contractor employees' participation in such training are not invoiced to the Solicitation.

3.6.10. Architecture and System Design

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall support the design and development of systems and associated enterprise architectures. The contractor shall provide all required architectural documentation in compliance with Department of Defense Architectural Framework (DoDAF) Enterprise Architecture guidance, IT Enterprise Architecture, or other guidance as specified in the Solicitation (such as AF SEAM).

3.6.11. Host Nation Installations

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

As specified by the Solicitation, the contractor shall use commercial telephone industry installation standards as documented in TL9000 compliant procedures for accomplishment of all installation work unless otherwise prohibited by host nation regulations and/or standards. The contractor shall determine if any host nation restrictions are applicable to any installation. The contractor shall be responsible for compliance with all host nation labor, safety, and environmental laws, regulations, and standards applicable at each installation location. If any additional permits or regulations apply, the contractor shall inform the Government and provide a proposal to initiate the appropriate documentation upon approval from the Government.

3.6.12. Tools and Test Equipment

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

Unless specified otherwise in the Solicitation, the contractor shall provide all tools and test equipment required to perform any required product installation and maintenance as called for by the Solicitation. All tools and test equipment shall remain the property of the contractor.

3.6.13. Warranty

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

Each product shall include a warranty as specified in Section I, Clause 52.246-17. In addition to FAR Clause 52.246-17, the following additional requirements apply: Users shall have highly reliable and maintainable network-centric products and system solutions to interoperate with the described environment. Components shall be maintainable by the user without voiding the warranty coverage. Components, which are expandable, shall be expandable by the user without voiding the warranty coverage provided the Government adheres to standard commercial practices in accomplishing the additions. Four types of warranty shall be provided:

1. System Warranty
2. Workmanship Warranty
3. Construction Warranty
4. Equipment Warranty

The warranty program shall provide for restoration of the system and repair of equipment in a timeframe specified in this contract, unless stated otherwise in the Solicitation. The Contractor shall provide means to transport equipment and bear transportation charges and responsibility for equipment and repair personnel under warranty while in transit both to and from the Government site.

3.6.14. System Warranty

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

Unless specified otherwise in the Solicitation, the Contractor shall provide a minimum one-year system warranty (some customers may require two or more years of warranty) to include coverage of all equipment supplied, installed, and integrated by the Contractor associated with delivery of infrastructure capabilities as defined by the AF enterprise architecture.. The system warranty shall ensure the full operational use of the system (CFE and GFE). The Contractor shall provide to the Government a 24-hour a day, 7-day a week point of contact for the system warranty. The system warranty shall begin at the time the final system DD Form 250 is signed by an authorized Government representative. The system warranty shall provide fault diagnosis, hardware and software repair, replacement, or redesign. The Contractor shall be responsible for diagnosing any problems, identifying malfunctioning equipment, and removing the equipment for repair. Prior approval shall be obtained from the authorized Government site representative before any GFE is removed from the system. Actual repair of malfunctioning GFE will be the responsibility of the Government, unless stated otherwise in the Solicitation. The system warranty shall include transportation for both Contractor personnel and equipment to and from the specific site. The system warranty shall provide for a return to service any malfunctioning CFE component or applications within 48 clock hours CONUS, 96 clock hours OCONUS after notification by the authorized Government site representative unless stated otherwise by the Solicitation. Costs for system warranty will be included within each Solicitation proposal provided by the contractor as required by the Solicitation.

In lieu of a system proposal that includes a traditional warranty, the Customer and Contractor may agree to a basic system proposal plus a block of hours for Contractor Maintenance Support Services. For many Contractors and Customers, this strategy has proven advantageous since traditional system warranties can be voided by today's dynamically changing networks forcing the Customer to maintain the network in a static environment during the warranty period. In addition, support is limited to a much narrower scope with a traditional system warranty whereas a Contractor Support Services contract is much more flexible in solving problems as they arise within the entire Network-Centric environment.

3.6.15. Workmanship Warranty

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

Unless specified otherwise in the Solicitation, the Contractor shall provide a minimum one year workmanship warranty (some customers may require two or more years of warranty) on all work provided or integrated under this contract. The warranty shall ensure the full operational use of the system (CFE and GFE). The Contractor shall provide to the Government a 24-hour a day, 7 day a week point of contact for the workmanship warranty. The workmanship warranty shall begin at the time the final system DD Form 250 is signed by an authorized Government representative. The workmanship warranty shall provide fault diagnosis, hardware and software repair, replacement, or redesign. The Contractor shall be responsible for diagnosing and fault isolation of any problems, identifying the poor workmanship causing the problem and affecting an acceptable industry standard repair. Prior approval shall be obtained from the authorized Government site representative before any GFE is removed from the system. Actual repair of malfunctioning GFE will be the responsibility of the Government. The workmanship system warranty shall include transportation for both Contractor personnel and bits, pieces, and parts to and from the specific site and the actual repair. The workmanship warranty shall provide for a return to service any malfunctioning CFE component or applications within 48 clock hours CONUS, 96 clock hours OCONUS after notification by the authorized Government site representative unless stated otherwise by the Solicitation.

3.6.16. Construction Warranty

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

Unless specified otherwise in the Solicitation, the Contractor shall provide a minimum one-year construction warranty (some customers may require two or more years of warranty) on all work provided or integrated under this contract. The warranty shall ensure the full operational use of all work. The Contractor shall provide to the Government a 24-hour a day, 7-day a week point of contact for the construction warranty. The construction warranty shall begin at the time the final system DD Form 250 is signed by an authorized Government representative. The construction warranty shall provide fault diagnosis, repair, replacement, or redesign. The Contractor shall be responsible for diagnosing and fault isolation of any degradation problems, identifying the poor construction-ship causing the problem and affecting an acceptable industry standard repair. Prior approval shall be obtained from the authorized Government site representative or Government COR before affecting any repair. The construction warranty shall include transportation for Contractor personnel, bits, pieces, and parts to and from the specific site and the actual repair. The construction warranty shall provide for a return to service any degrading component or area within 48 clock hours CONUS, 96 clock hours OCONUS after notification by the authorized Government site representative unless stated otherwise by the Solicitation.

3.6.17. Equipment Warranty

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

Unless specified otherwise in the Solicitation, the Contractor shall provide standard, OEM pass through, extended or otherwise warranties for the periods specified in the Solicitation for all hardware and software products, for both CONUS and OCONUS Government sites located worldwide. Repairs shall be accomplished within 48 clock hours CONUS, 96 clock hours OCONUS of receipt of the equipment warranty trouble call, unless stated otherwise by the Solicitation, when the Contractor is performing the warranty repair. The warranty shall also provide for repair or replacement of equipment and repair and distribution of updated software to all users who purchased the software from this contract. Warranty coverage commences on the date of acceptance in block 21B of the DD Form 250, Commercial Invoice dated and signed, or SF 1449 dated and signed.

The Contractor shall provide a worldwide warranty repair solution capability for systems with qualified maintenance repair personnel and leverage existing OEM support infrastructures to the greatest extent possible. Repairs shall be performed at a time required by the Task/Delivery

Order/Delivery Order or as coordinated by the Government COR. The Contractor shall provide a 24-hour, 7-day a week warranty repair point of contact to receive calls from the Government. The Contractor shall provide the capability for toll-free telephone access for obtaining technical warranty repair support assistance from worldwide locations. The Contractor shall provide the tools, equipment and consumables required for personnel to complete their duties. The Contractor shall not invalidate the warranty provided on components purchased under this contract when the Government elects to perform user self-maintenance and/or self-installation during the warranty period. Note: The Government will perform routine user-maintenance for all equipment both during and after the warranty period using separately orderable spare parts and/or repaired parts from this contract. The Government will only be liable for any damage to the equipment that results from Government Maintenance or additions to equipment that did not adhere to stand commercial practice. At no additional charge to the Government, the Contractor shall furnish, for hardware purchased under this contract, all repairs (labor and parts) for the duration of the warranty period. At a minimum, repair during the warranty period shall be equivalent to standard per-call maintenance during the principal period of maintenance (PPM) as specified in this PWS. The Government, at its option, may order additional repair coverage during the warranty period. The Governments purchase of additional repair coverage will be specified in details by the Solicitation.

All parts replaced during the warranty period, in an unclassified environment, shall become the property of the Contractor. However, in classified environments the Government will maintain title of certain items. These items typically will be broken storage devices/mediums. All other parts may be returned to the contractor and the government will have up to 30 days to relinquish possession of the part.

The warranty shall not apply to maintenance required due to the fault or negligence of the Government. If Government negligence results in a repair call (either for equipment under warranty or per call maintenance), the maximum repair time shall not apply and the Government will pay the price per hour specified in the contract for the hours rendered to complete the repair.

Only new or reconditioned parts shall be provided for repairs. If reconditioned parts are provided, the reconditioned parts shall carry the same warranty provisions as originally provided by the Contractor for new parts.

The Contractor guarantees to repair at no charge any malfunction which reoccurs within 90 calendar days of the initial repair. Warranty of Repair is a separate warranty from those described elsewhere in the contract.

If the Contractor elects to replace the malfunctioning hardware, the Contractor shall either provide the Government with a permanent replacement which shall contain a unique serial number or shall provide the Government with a temporary replacement with a unique serial number. If the Contractor elects to repair the malfunctioning hardware, the Contractor shall repair and return the repaired hardware to the Government at which time the temporary replacement shall be surrendered to the Contractor at the contractor's expense.

3.6.18. Maintenance

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

Unless specified otherwise in the Solicitation, the contractor shall provide a worldwide maintenance solution capability (on-site and on-site per-call) for systems provided under this contract with qualified maintenance personnel, leveraging existing OEM support infrastructures to the greatest extent possible. Maintenance shall be performed at a time required by the Solicitation or as coordinated by the Government COR. The contractor shall provide a maintenance POC 24-hours-a-day, 7-days-a-week to receive calls from the Government. The specific maintenance requirements will be included in the Solicitation and may include maintenance on systems/equipment not purchased under this contract. The contractor shall provide the capability for toll-free telephone and e-mail access for obtaining technical maintenance support assistance from worldwide locations. The contractor shall provide remote engineering and technical support via telephone or other remote system capabilities to assist maintenance personnel, analyze software, hardware, system problems and provide problem resolutions. This support may consist of routine maintenance, testing, diagnostic fault isolation, problem resolution, activation of features and/or equipment, software configurations and general information on features or capabilities of equipment. All requests for remote maintenance services shall be acted upon immediately upon receipt of the request and logged for inclusion in a service ticket status log of some type. The requesting unit shall be notified of the current status of corrective actions for hardware and software related problems that cannot be immediately corrected. The contractor shall provide the tools, equipment and consumables required for personnel to complete their duties.

3.6.19. Per-Call Maintenance/Standard Per-Call Maintenance (SPCM)

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

Unless specified otherwise in the Solicitation, the contractor shall provide the Government with on-site per-call maintenance at the Government location for all cable plant and non-cable plant items. One instance of a per-call maintenance visit shall include the repair of all units identified at the time the Government notification call to the vendor was placed. The minimum charge per-call shall not exceed one (1) labor hour. The maximum charge per-call shall not exceed any limitations (labor and parts) indicated by the Government at the time of the maintenance call without prior approval from the designated Government official and as funded in the applicable Solicitation. Hourly rate charges shall commence when the contractor representative reports to the Government site representative indicated in the call. Outside the Principal Period of Maintenance (OPPM) is defined as all-time other than the PPM. If a call is placed during the OPPM or, if the Government wants the weekend/holiday time to count toward time to repair, then the OPPM rate may be applicable. The OPPM rate shall be applicable only if specifically requested by the Government at the time of the maintenance call and approved by the contracting officer.

3.6.20. Contractor Provided Non-Cable Plant, Non-Switching System SPCM

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

Unless specified otherwise in, the contractor shall have, from the time of notification of equipment failure(s), a maximum of 8 hours to respond and 48 hours to complete the repair(s) or replace (at the user's site) the malfunctioning system(s) or components for CONUS or 16 hours to respond and 96 hours to complete the repair(s) or replace (at the user's site) the malfunctioning system(s) or components for OCONUS, unless otherwise stated in the Solicitation.

3.6.21. Government Owned Equipment Non-Cable Plant, Non-Switching System SPCM

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

Unless specified otherwise in the Solicitation, the contractor shall maintain the non-cable plant and non-switching systems (i.e., microwave radios, UPS equipment, multiplexers, antennas, LAN/CAN/MAN/WAN equipment, VTC equipment, phones, land mobile radios (LMR) Air Traffic Control and Landing Systems (ATCALS) and Meteorological and Navigational Aid (METNAV)) and those provided by the contractor under this contract. The contractor shall have, from the time of notification of equipment failure(s), a maximum of 8 hours to respond and 48 hours to complete the repair(s) or replace (at the user's site) the malfunctioning system(s) or components for CONUS or 16 hours to respond and 96 hours to complete the repair(s) or replace (at the user's site) the malfunctioning system(s) or components for OCONUS, unless otherwise stated in the Solicitation.

3.6.22. Switching System SPCM

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

Unless specified otherwise in the Solicitation, the contractor shall have, from the time of notification of equipment failure(s), a maximum of 4 hours to respond and 24 hours to complete the repair(s) or replace (at the user's site) the malfunctioning system(s) or components for CONUS or 8 hours to respond and 72 hours to complete the repair(s) or replace (at the user's site) the malfunctioning system(s) or components for OCONUS, unless otherwise stated in the Solicitation (i.e., non-ISDN/ISDN capable, DSS, etc.).

3.6.23. Cable Plant Maintenance

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

Unless specified otherwise in the Solicitation, the contractor shall have, from the time of notification of equipment failure(s), a maximum of 2 hours to respond and 8 hours to complete the repair(s) or temporarily replace or patch the malfunctioning components for CONUS or 4 hours to respond and 12 hours to complete the repair(s) or temporarily replace or patch the malfunctioning components for OCONUS, unless otherwise stated in the Solicitation. This maintenance shall include inside and outside cable plant maintenance. If the Government cannot provide drawings identifying placement of both inside and outside cable components to be maintained, then the Government will order a cable-plant survey via Solicitation using the applicable labor categories; the contractor shall not be held accountable for any repair timeframes until the Government provides such drawings. The contractor shall also provide, on a pre-scheduled basis, preventative and routine maintenance required for optimized usage and life of the existing cable plant on a per-call basis. Within 24 hours of a repair or patch that restores service using a temporary repair, the contractor shall provide the Government with a draft list for components that were temporarily repaired until permanent replacements could be obtained. In this event, the contractor shall provide a firm-fixed-price proposal to the user for installation of the components identified in the draft list.

3.6.24. Rapid Response Per-Call Maintenance (RRPCM)

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

For RRPCM, the contractor shall have a maximum time of 2 hours from the time of notification of failure(s) to respond, unless stated otherwise in the Solicitation. Repair time shall be within 12 hours.

3.6.25. System Maintenance

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

Unless specified otherwise in the Solicitation, the contractor shall provide all supplies, parts, tools, and test equipment required for maintenance of the system and be responsible for total system maintenance.

3.6.26. Maintenance Charges

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The per-call maintenance charge may include the CLIN labor rate, travel and ODCs, and transportation of any equipment, as applicable. Replaced faulty parts shall remain the property of the Government.

3.6.27. Maintenance Alternative

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The Government may select maintenance alternative (standard or rapid per call response) with the issuance of a Solicitation. The Government shall have the option to change the type of maintenance by giving the contractor thirty (30) days notice and a contract modification. Any change in type of maintenance will not be considered a partial termination of the Solicitation for the convenience of the Government.

3.6.28. Relocation and Removal

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

The contractor shall relocate and remove systems as specified in the Solicitation. The contractor shall be responsible for storage, staging and deployment of any equipment and materials provided as part of awarded Solicitations unless otherwise mutually agreed upon by the contractor and the Government. If removal of equipment and/or material is necessary, the contractor shall be responsible for disposal and shall comply with all applicable industry rules and regulations. Any equipment removal and/or disposal shall be coordinated with a designated official at the host base communications squadron.

3.6.29. Surge Requirements

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

Surge requirements include greater than expected requirements/workload for existing services within the scope of Solicitations awarded. Normally, surge requirements are of short duration, from one to six months. An example of a surge requirement is additional help desk or system maintenance support personnel required to handle temporarily increased workloads because of war or contingency. Surge requirements shall be accomplished as required under the Solicitation.

3.6.30. Unified Capabilities Requirements (UCR)

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

Unless specified otherwise in the Solicitation, the contractor shall report to the government through quarterly PMRs, how each solution awarded meets the Unified Capabilities Requirements (UCR). Detail shall include, but not be limited to the applicable MILDEP Service Level Architecture requirements. For example, vendor shall report how each awarded solution that is implemented at a United States Air Force Installation meets the United States Air Force i-TRM Architecture requirements. Similar report requirements including the ConstellationNet Architecture may also be requested at the Solicitation level.

3.6.31. Special Asset Tagging

[Sample language below. Modify to fit your requirement. Delete if not applicable.]

When required and defined by the Delivery/Solicitation, the contractor shall provide special asset tags IAW DODI8320.04, Item Unique Identification (IUID) Standards for Tangible Personal Property, to include Unique Identification (UID) tagging requested by non-DoD customers.

3.7. [Next Requirement]

4. Contractual Requirements

[The following contract requirements are applicable to all Solicitations. Each requirement should be tailored to fit your Solicitation.]

4.1. Performance Reporting

[Modify to fit your Solicitation. Sample language below.]

The contractor's performance will be monitored by the Government and reported in Contractor Performance Assessment Reporting (CPARs). Performance standards shall include the contractor's ability to:

1. Provide quality products, incidentals and customer support;
2. Meet customer's agreed-upon timelines for scheduled delivery of items, warranty, and/or incidental services: Emergency/critical, Maintenance/Warranty – 24 x 7 x 365, and remote OCONUS, OCONUS vs. CONUS response times;
3. Provide satisfactory product repairs or advance replacement, as appropriate;
4. Provide timely and accurate reports;
5. Respond to the customer's requests for proposals and configuration assistance as identified in each delivery order; and
6. Meet subcontracting goals.

4.2. Program Management

[Modify to fit your Solicitation. Sample language below.]

The contractor shall identify a Program Manager who shall be the primary representative responsible for all work awarded under this contract, participating in Program Management Reviews and ensuring all standards referenced herein are adhered to.

4.2.1. Services Delivery Summary

[Modify to fit Solicitation level service/performance parameters. Make sure the services required have measurable outcomes. Please refer to Appendix N3, "Network Operations and Infrastructure Solutions Performance Metrics," for minimum and recommended performance outcomes.]

The Services Delivery Summary (SDS) will be in accordance with AFI 63-101, Acquisition and Sustainment Life Cycle Management and FAR Subpart 37.6, Performance-Based Acquisition. Service Level Agreements (SLAs) will be defined in each Solicitation.

[Modify to fit your Solicitation. Example Table below.]

Desired Outcome		Performance Objective	Performance Threshold	
Overall Outcome	Specific Outcomes		Target	Tolerance
Compliance with NetOps and Infrastructure Solutions support requirements (delivery, quality)	Ensure compliance with NetOps and Infrastructure Solutions deliverables requirements	Deliver the NetOps and Infrastructure Solutions w/ predetermined outcomes and on time	Documentation submitted IAW CDRL A001 verifies the Solicitation was completed on time	98% of the time

4.2.2. Solicitation Management

[Modify to fit your Solicitation. Sample language below.]

The contractor shall establish and provide a qualified workforce capable of performing the required tasks. The workforce may include a project/Solicitation manager who will oversee all aspects of the Solicitation. The contractor shall use key performance parameters to monitor work performance, measure results, ensure delivery of contracted product deliverables and services, support management and decision-making and facilitate communications. The contractor shall identify risks, resolve problems and verify effectiveness of corrective actions. The contractor shall institute and maintain a process that ensures problems and action items discussed with the Government are tracked through resolution and shall provide timely status reporting. Results of contractor actions taken to improve performance should be tracked, and lessons learned incorporated into applicable processes. The contractor shall establish and maintain a documented set of disciplined, mature, and continuously improving processes for administering all contract and Solicitation efforts with an emphasis on cost-efficiency, schedule, performance, responsiveness, and consistently high-quality delivery.

4.2.3. Configuration and Data Management

[Modify to fit your Solicitation. Sample language below.]

The Contractor shall establish, maintain, and administer an integrated data management system for collection, control, publishing, and delivery of all program documents. The data management system shall include but not be limited to the following types of documents: CDRLs, White Papers, Status Reports, Audit Reports, Agendas, Presentation Materials, Minutes, Contract Letters, and Solicitation Proposals. The contractor shall provide the Government with electronic access to this data, including access to printable reports. The contractor shall have an approved property control system IAW FAR 45, DFARS 245, and approved procedures to document and track all GFM and Government Furnished Equipment (GFE). The contractor shall provide as-built documentation including, but not limited to, drawings and diagrams of the solution provided under each Solicitation identifying specific cards in a chassis/shelf. The as-built documentation shall also include layout drawings, power drawings/specifications, floor plans and engineering specifications generated in support of the installation of the system. Documentation shall also include equipment listing with serial/model numbers, and manufacturer specifications.

4.2.4. Records, Files and Documents

[Modify to fit your Solicitation. Sample language below.]

All physical records, files, documents, and work papers, provided and/or generated by the Government and/or generated for the Government in performance of this PWS, maintained by the Contractor which are to be transferred or released to the Government or successor Contractor, shall become and remain Government property and shall be maintained and disposed of IAW AFMAN 33-363, Management of Records; AFI 33-364, Records Disposition – Procedures and Responsibilities; the Federal Acquisition Regulation, and/or the Defense Federal Acquisition Regulation Supplement, as applicable. Nothing in this section alters the rights of the Government or the Contractor with respect to patents, data rights, copyrights, or any other intellectual property or proprietary information as set forth in any other part of this PWS or the Network Operation (NetOps) and Infrastructure Solutions contract of which this PWS is a part (including all clauses that are or shall be included or incorporated by reference into that contract).

4.3. Security Management

4.3.1. Safeguarding Classified Information

[Modify to fit your Solicitation. Sample language below.]

The contractor shall transmit and deliver classified material/reports IAW the National Industrial Security Program Operations Manual (NISPOM) and the National Industrial Security Program Operating Manual (DoD 5220.22-M). These requirements shall be accomplished as specified in the Solicitation. All Classified Contracts must have at a minimum, the Clause 52.204-2 Security Requirement, incorporated into the contract.

Each Base will follow its own classified process IAW with the proscribed Federal guidance of the NISPOM and FAR "Subpart 4.4 along with DD Form 254. When transmitting classified information ensure all classified information is properly sanitized and/or degaussed of all sensitive/classified information IAW AFSSI 5020.

For assistance and guidance on submitting Classified Solicitations, the Netcentric Customer Service can be reached at COMM 334-416-5070 / DSN 312-596-5070 Option 1.

4.3.2. Personnel Security

[Modify to fit your Solicitation. Sample language below.]

Individuals performing work under these Solicitations shall comply with applicable program security requirements as stated in the Solicitation. NETCENTRIC will support the following levels of security: Unclassified; Unclassified, But Sensitive; Secret (S); Secret Sensitive Compartmented Information (S/SCI); Top Secret (TS); and Top Secret Sensitive Compartmented Information (TS/SCI)

Certain Solicitations may require personnel security clearances up to and including Top Secret and certain Solicitations may require all employees to be United States citizens. The security clearance requirements will depend on the security level required by the proposed Solicitation. The Solicitations may also require access to sensitive compartmented information (SCI) for which SCI eligibility will be required. Contractors shall be able to obtain adequate security clearances prior to performing services under the Solicitation. The Contract Security Classification Specification (DD Form 254) will be at the basic contract and Solicitation level and will encompass all security requirements. All contractors located on military installations shall also comply with Operations Security (OPSEC) requirements as set forth in DoD Directive 5205.02, Operations Security Program and AFI 10-701, Operations Security. In accordance with DoD 5200.2-R, Personnel Security Program (Jan 87), DoD military, civilian, consultants, and contractor personnel using unclassified automated information systems, including e-mail, shall have, at a minimum, a completed favorable National Agency Check plus Written Inquiries (NACI).

The types of Personnel Security Investigations (PSI) required for the contractor vary in scope of investigative effort depending upon requirements of the Government and/or conditions of the contract/Solicitation. In cases where access to systems such as e-mail is a requirement of the Government, application/cost for the PSI shall be the responsibility of the Government. In cases where access to systems is as a condition of the contract/Solicitation, application/cost for the appropriate PSI shall be the responsibility of the contractor. In such instances the contractor shall diligently pursue obtaining the appropriate PSI for its employees prior to assigning them to work any active Solicitation.. Acquisition planning must consider antiterrorism (AT) measures when the effort to be contracted could affect the security of operating forces (particularly in-transit forces), information systems and communications systems IAW DoD Instructions 2000.16 Anti-Terrorism Standards.

4.3.3. Protection of System Data

[Modify to fit your Solicitation. Sample language below.]

Unless otherwise stated in the Solicitation, the contractor shall protect system design-related documents and operational data whether in written form or in electronic form via a network in accordance with all applicable policies and procedures for such data, including DOD Regulations 5400.7-R and DoDM 5200.01 to include latest changes, and applicable service/agency/ combatant command policies and procedures. The contractor shall protect system design related documents and operational data at least to the level provided by Secure Sockets Layer (SSL)/Transport Security Layer (TSL)-protected web site connections with certificate and or user id/password-based access controls. In either case, the certificates used by the Contractor for these protections shall be DoD or IC approved Public Key Infrastructure (PKI) certificates issued by a DoD or IC approved External Certification Authority (ECA) and shall make use of at least 128-bit encryption.

4.3.4. On-Site Task Approval Process

[Modify to fit your Solicitation. Sample language below.]

The contractor shall, for CONUS tasks (7-day notice) and for OCONUS tasks (14-day notice), notify the on-site COR in writing before a requirements analysis/conceptual design visit, site survey, and other on-site tasks are to be performed. The following information must be provided; Names of Employees, SSAN, Security Clearance, Location, Project Number, On/About Date Planned for On-Site Work, Anticipated Duration of Visit, Support Required.

4.3.5. Travel Requirements

[Modify to fit your Solicitation. Sample language below.]

The contractor shall coordinate specific travel arrangements with the individual Contracting Officer or Contracting Officer’s Representative to obtain advance, written approval for the travel about to be conducted. The contractor’s request for travel shall be in writing and contain the dates, locations, and estimated costs of the travel in accordance with the basic contract clause H047.

If any travel arrangements cause additional costs to the Solicitation that exceed those previously negotiated, written approval by CO is required, prior to undertaking such travel. Costs associated with contractor travel shall be in accordance with FAR Part 31.205-46, Travel Costs. The contractor shall travel using the lower cost mode transportation commensurate with the mission requirements. When necessary to use air travel, the contractor shall use the tourist class, economy class, or similar accommodations to the extent they are available and commensurate with the mission requirements. Travel will be reimbursed on a cost reimbursable basis; no profit or fee will be paid.

4.3.6. Other Direct Cost (ODC)

[Modify to fit your Solicitation. Sample language below.]

The contractor shall identify ODC and miscellaneous items as specified in each Solicitation. No profit or fee will be added; however, DCAA approved burden rates are authorized.

4.4. [Next Requirement]

5. Deliverables

The Government requires all deliverables that include Scientific and Technical Information (STINFO), as determined by the Government, be properly marked IAW DoDI 5230.24 and AFI 61-204 prior to initial coordination or final delivery. Failure to mark deliverables as instructed by the government will result in non-compliance and non-acceptance of the deliverable. The contractor will include the proper markings on any deliverable deemed STINFO regardless of media type, stage of completeness, or method of distribution. Therefore, even draft documents containing STINFO and STINFO sent via e-mail require correct markings. Additionally, as required by individual Task/Delivery Orders, the contractor shall formally deliver as a CDRL all intellectual property, software, licensing, physical records, files, documents, working papers, and other data for which the Government shall treat as deliverable.

6. Quality Processes

[Modify to fit your Solicitation. Sample language below.]

As a minimum, the prime contractor shall be appraised at least Level 2 or higher for CMMI Development by a Software Engineering Institute (SEI) or ISO 9001:2000 or ISO 9001:2008 or ISO/IEC 20000 for the entire performance period of the contract, inclusive of options. This certification must be held at the prime offeror's organizational level performing the contract.

[Modify to fit your Solicitation. Sample language below.]

As a minimum, the prime contractor shall be appraised at ISO 9001:2000 or ISO 9001:2008 or ISO/IEC 20000 or CMMI Development Level 2 (or higher) using the Software Engineering Institute's (SEI) SCAMPI A method by an SEI-authorized lead appraiser, or comparable documented systems engineering processes, for the entire performance period of the contract, inclusive of options. Formal certifications must be held at the prime offeror's organizational level performing the contract. If not ISO certified or SEI appraised, acceptable comparable Systems Engineering (SE) processes shall be maintained for the entire performance period of the contract, inclusive of options. These processes include: requirements management; configuration management; development of specifications; definition and illustration of architectures and interfaces; design; test and evaluation/verification and validation; deployment and maintenance The Government reserves the right to audit and/or request proof of these comparable quality processes for the entire performance period of the contract, inclusive of options.

In addition, small business companion contract awardees that elect to take advantage of provisions outlined in clause H139 must comply with the quality processes requirements. This means that at the time of award and as a minimum, the prime contractor shall be appraised at ISO 9001:2000 or ISO 9001:2008 or ISO/IEC 20000 or CMMI Development Level 2 (or higher) using the Software Engineering Institute's (SEI) SCAMPI A method by an SEI-authorized lead appraiser and must be held at the prime offeror's organizational level performing the contract for the entire performance period of the contract, inclusive of options. Evidence of comparable Systems Engineering (SE) processes will not be accepted.

7. Applicable Documents and Standards

[Refer to Appendix N5, "Network Operations and Infrastructure Solutions Standards and Documentation" for the applicable certifications, specifications, standards, policies and procedures represent documents and standards that may be placed on individual contract Solicitations. Tailor the below list as needed (add or delete requirements). Individual Solicitations may impose additional standards to those required at the contract level. The list below is not all-inclusive and the most current version of the document at the time of Solicitation issuance will take precedence. Web links are provided wherever possible.]

8. Products Standards and Compliance Requirements

[Tailor this list of products standards and compliance requirements depending on the required hardware and software required of this Solicitation.]

Information Assurance (IA) Technical Considerations

The contractor shall provide Commercial-Off-The-Shelf (COTS) IA and IA-enabled products IAW AFI 33-200, Information Assurance. These products must be National Security Telecommunications and Information Systems Security Policy Number 11 (NSTISSP-11) compliant, requiring them to be validated by accredited labs under the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme or National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Cryptographic Module Validation Program (CMVP). The following are some examples of IA and IA enabled devices: data/network encryptors, intrusion detection devices such as Firewalls, Intrusion Detection System, Authentication Servers, Security Gateways, High Assurance IP encryptor and Virtual Private Networks.

DoD IPV6 Requirement

All Products must meet the criteria in DoD IPv6 Standard Profiles for IPv6 Capable Products version 5.0 July 2010 (http://jitc.fhu.disa.mil/apl/ipv6/pdf/disr_ipv6_50.pdf). Some example IPV6 mandated products from the DoD IPV6 Standards Profile are listed below:

- Host/Workstations - a desktop or other end-user computer or workstations running a general purpose operating system such as UNIX, Linux, Windows, or a proprietary operations system that is capable of supporting multiple applications.

- Network Appliance or Simple Server - Simple end nodes such as cameras, sensors, automation controllers, networked phones or adapters such as Circuit-to-Packet (CTP) devices, typically with an embedded operating system and specialized software for limited applications. A Network Appliance is typically managed by an end-user, but may support more than one concurrent user remotely via a Web browser interface. A Simple Server supports a small number of concurrent clients via a web browser interface or other protocol with a client application. Examples of simple servers are stand-alone network print servers, storage servers, Session Initiation Protocol (SIP)11 servers, a "web camera" appliance that serves pictures via an embedded web server, and a network time server appliance that solely functions to serve NTP requests. Advanced Server - End Nodes with one or more server-side applications (for example Dynamic Host Configuration Protocol (DHCPv6), Domain Name Server (DNS), Network Time Protocol (NTP), E-mail, File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), web server, storage server or database) to support clients in the network

- Intermediate Nodes – Routers, Switches, IA or IA enabled devices

- IPV6 Capable Software - a product that implements functions available via an IPv6 interface to end-users, network nodes or other software, when installed on an appropriate hardware platform.

Energy Star

All applicable Products must be EnergyStar® compliant per DoDI 4170.11 and FAR Part 52.223-153.

ENERGY EFFICIENCY IN ENERGY-CONSUMING PRODUCTS (DEC 2007)

(a) Definition: As used in this clause, "Energy-efficient product"…
(1) Means a product that—
(i) Meets Department of Energy and Environmental Protection Agency criteria for use of the Energy Star® trademark label; or
(ii) Is in the upper 25 percent of efficiency for all similar products as designated by the Department of Energy's Federal Energy Management Program.

(2) The term "product" does not include any energy-consuming product or system designed or procured for combat or combat-related missions (42 U.S.C. 8259b).

(b) The Contractor shall ensure that energy-consuming products are energy efficient products i.e., ENERGY STAR products or FEMP-designated products) at the time of contract award, for products that are—
(1) Delivered;
(2) Acquired by the Contractor for use in performing services at a Federally-controlled facility;
(3) Furnished by the Contractor for use by the Government; or
(4) Specified in the design of a building or work, or incorporated during its construction, renovation, or maintenance.

(c) The requirements of paragraph (b) apply to the Contractor (including any subcontractor) unless—
(1) The energy-consuming product is not listed in the ENERGY STAR Program or FEMP; or
(2) Otherwise approved in writing by the Contracting Officer.

(d) Information about these products is available for—
(1) ENERGY STAR at http://www.energystar.gov/products; and
(2) FEMP at www.femp.energy.gov/technologies/eep_purchasingspecs.html.

NOTE: Remove if not applicable. The following are some example products that are required to be energy star compliant: computers, displays and monitors, enterprise servers, copiers, digital duplicators, fax/printer machines, printers, scanners, televisions, cordless phones, battery chargers, set-top and cable boxes, and audio and video equipment. For further guidance please see the below url: http://www1.eere.energy.gov/femp/technologies/eep_purchasingspecs.html

Encryption Mandates

All Products that will perform any type of data encryption, it is required that the encryption method being used meets FIPS standards for both information assurance and interoperability testing. For more information on FIPS, go to: http://www.itl.nist.gov/fipspubs/by-num.htm. Some example FIPS standards would be FIPS 201 which specifies the architecture and technical requirements for a common identifications standard for Federal employees and contractors (i.e. Common Access Card). Another one is FIPS 140-2 which specifies the security requirements that will be satisfied by a cryptographic module (i.e. the underlying algorithms to process information).

BIOS Mandate

All Products shall be BIOS protection compliant with Section 3.1 “Security Guidelines for System BIOS Implementations of SP 800-147,” per DoD CIO, in order to prevent the unauthorized modification of BIOS firmware on computer systems.

Biometric Mandate

All Biometric products shall be built to the DoD Electronic Biometric Transmission Specification (EBTS) version 3.0 standard. For more information please visit the Biometric Identity Management Agency website at: http://www.biometrics.dod.mil/.

Special Asset Tagging

The contractor shall provide special asset tags IAW DODI 8320.04, Item Unique Identification (IUID) Standards for Tangible Personal Property, to Include Unique Identification (UID) tagging requested by non-DoD customers. NOTE: Remove if not applicable. If the following criteria apply then leave the above statement in your SOO. All items for which the Government's unit acquisition cost is $5,000 or more;

- Items for which the Government's unit acquisition cost is less than $5,000, when identified by the requiring activity as DoD serially managed, mission essential or controlled inventory;
- When the Government's unit acquisition cost is less than $5,000 and the requiring activity determines that permanent identification is required;
- Regardless of value, (a) any DoD serially managed subassembly, component, or part embedded within an item and, (b) the parent item that contains the embedded subassembly, component or part.

If you require further guidance on Special Asset Tagging please see DoDI 8320.04 at: http://www.dtic.mil/whs/directives/corres/pdf/832004p.pdf.

Software Tagging

Commercial off-the-shelf software items shall support International Standard for Software Tagging and Identification, ISO/IEC 19770-2, Software Tags when designated as mandatory by the standard. NOTE: Check ISO/IEC 19770-2 to see if Software Tagging applies to this acquisition. Some examples of when you might require software tagging would be if you needed to record unique information about an installed software application or to support software inventory and asset management. For more information please go to http://tagvault.org/.

Radio Frequency Identification (RFID)

The contractor shall provide RFID tagging IAW DoD Radio Frequency Identification (RFID) Policy, 30 July 2004 or most current version. NOTE: Check RFID Policy, 30 July 2004 at: https://acc.dau.mil/adl/en-S/142796/file/27748/ RFIDPolicy07-30-2004.pdf to see if Special Asset Tagging applies to this acquisition. Some example uses of RFID are when tags are placed into freights containers, ammunition shipments, or attached to unit level IT equipment to facilitate accountability.

Section 508 of the Rehabilitation Act

The Contractor shall meet the requirements of the Access Board's regulations at 36 CFR Part 1194, particularly 1194.22, which implements Section 508 of the Rehabilitation Act of 1973, as amended. Section 508 (as amended) of the Rehabilitation Act of 1973 (20 U.S.C. 794d) established comprehensive requirements to ensure: (1) Federal employees with disabilities are able to use information technology to do their jobs, and (2) members of the public with disabilities who are seeking information from Federal sources will be able to use information technology to access the information on an equal footing with people who do not have disabilities.

Hardware and Associated Software and Peripherals

All hardware delivered under this DO shall include associated software, documentation and associated peripherals required for operations (such as controllers, connectors, cables, drivers, adapters, etc.) as provided by the Original Equipment Manufacturer (OEM). This is true only if the applicable OEM provides such items with the product itself.

Authorized Resellers

The contractor may be an authorized reseller of new and refurbished/remanufactured equipment for OEMs proposed under this DO. The contractor may also procure directly from the OEM or utilize other legitimate distribution channels to provide the required products. Any contractor’s channel relationships with their OEM partners (gold, silver, etc) will be represented in the best pricing offered. DOs may restrict the use of authorized resellers, specific OEMs, or identify required OEMs. Any product offering that is remanufactured or refurbished shall be clearly identified as such by the contractor. Remanufactured products shall have the OEM or factory certification if available for that product.

Technical Refresh

In order to ensure new design enhancements and technological updates or advances, the contractor shall offer, under this DO, hardware and software components available to the contractor's commercial customers. Furthermore, the contractor shall make available any commercially available updates to the hardware and software provided under this DO. If such updates are available to other customers without charge, then they shall also be made available to the Government without additional charge. The contractor will ship these updates to existing customers who have acquired the hardware/software being updated under this DO. Vendor commercial product offerings shall include “state of the art” technology, i.e., the most current proven level of development available in each product category.

Trade Agreement Act (TAA)

All proposed products must be compliant with the Trade Agreements Act of 1979 (TAA) and related clauses in Section I of this contract. In accordance with DFARS 252.225-7021, the Trade Agreements Certificate at DFARS 252.225-7020 shall be provided for each end item defined and specified in a solicitation that exceeds the TAA threshold subject to the waivers and exceptions provided in FAR 25.4, and DFARS 225.4 offered in response to any RFQ issued under this contract. Please note that Federal Acquisition Regulation (FAR) paragraph 25.103(e) includes an exemption from the Buy American Act (BAA) for acquisition of information technology that are commercial items.

Items on Backorder

In their response to a Request for Quote (RFQ), the contractor shall provide notification, if applicable, that a particular item is on backorder, the expected lead-time to fulfill the order, etc. It shall be implicit that a response to an RFQ with no items identified on backorder is a declaration that the items are available at the time of quote submission.

Warranty

The contractor shall provide any OEM pass through warranty and standard commercial warranties applicable to the products being purchased at no cost. This shall apply to new, refurbished and remanufactured equipment.

Customer Support

The prime contractor shall provide 24x7 live telephone support during the warranty period to assist in isolating, identifying, and repairing software and hardware failures, or to act as liaison with the manufacturer in the event that the customer requires assistance in contacting or dealing with the manufacturer.

Appendix N3 NetOps and Infrastructure Solutions Compliance and Standards List

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
1.	Section 508 of the Rehabilitation Act of 1973	http://www.opm.gov/html/508-textOfLaw.asp	On August 7, 1998, President Clinton signed into law the Rehabilitation Act Amendments of 1998 which covers access to federally funded programs and services. The law strengthens section 508 of the Rehabilitation Act and requires access to electronic and information technology provided by the Federal government. The law applies to all Federal agencies when they develop, procure, maintain, or use electronic and information technology. Federal agencies must ensure that this technology is accessible to employees and members of the public with disabilities to the extent it does not pose an "undue burden." Section 508 speaks to various means for disseminating information, including computers, software, and electronic office equipment. It applies to, but is not solely focused on, Federal pages on the Internet or the World Wide Web.
2.	DoDI 8520.02 Public Key Infrastructure (PKI) and Public Key (PK) Enabling	http://www.dtic.mil/whs/directives/corres/pdf/852002p.pdf	This instruction establishes and implements policy, assign responsibilities, and prescribe procedures for developing and implementing a DoD-wide PKI and enhancing the security of DoD information systems by enabling these systems to use PKI for authentication, digital signatures, and encryption.
3.	DFARS 252.227-7013 Rights in Technical Data---Non-commercial Items	https://acc.dau.mil/CommunityBrowser.aspx?id=33757	Provides guidelines for rights in technical data on non-commercial items.
4.	DODD 8320.02, Data Sharing in a Net-Centric Department of Defense	http://www.dtic.mil/whs/directives/corres/pdf/832002p.pdf	Establishes policies and responsibilities to implement data sharing, in accordance with Department of Defense Chief Information Officer Memorandum, “DoD Net-Centric Data Strategy,” May 9, 2003, throughout the Department of Defense. Directs the use of resources to implement data sharing among information capabilities, services, processes, and personnel interconnected within the Global Information Grid (GIG), as defined in DoD Directive 8100.1, “Global Information Grid (GIG) Overarching Policy,” September 19, 2002.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
5.	DoD Global Information Grid Architectural Vision	http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA484389&Location=U2&doc=GetTRDoc	The security challenges of the 21st century are characterized by change and uncertainty. Operations vary widely and partners cannot be anticipated. However, we are confronting that uncertainty by becoming more agile. Greater levels of agility rest upon leveraging the power of information – the centerpiece of today's Defense transformation to net-centric operations (NCO). Our forces must have access to timely and trusted information. And, we must be able to quickly and seamlessly share information with our partners, both known and unanticipated. The GIG Architectural Vision is key to creating the information sharing environment and will be critical to transformation to NCO.
6.	DoD Manual 5200.01, DoD Information Security Program: Overview, Classification, and Declassification, V1-V4	http://www.dtic.mil/whs/directives/corres/pdf/520001_vol1.pdf	The purpose of this manual is to implement policy, assign responsibilities, and provide procedures for the designation, marking, protection, and dissemination of controlled unclassified information (CUI) and classified information, including information categorized as collateral, sensitive compartmented information (SCI), and Special Access Program (SAP).
7.	DoD Metadata Registry	http://metadata.ces.mil/dse/irs/DDMS/	As part of the overall DoD Net-Centric Data Strategy, the DoD CIO established the DoD Metadata Registry (http://metadata.ces.mil) and a related metadata registration process for the collection, storage and dissemination of structural metadata information resources (schemas, data elements, attributes, document type definitions, style-sheets, data structures, etc.). This Web-based repository is designed to also act as a clearinghouse through which industry and government coordination on metadata technology and related metadata issues can be advanced. As OASD's Executive Agent, DISA maintains and operates the DoD Metadata Registry and Clearinghouse under the direction and Metadata Registry and Clearinghouse under the direction and Metadata Registry and Clearinghouse under the direction and Metadata Registry and Clearinghouse under the direction and oversight of OASD(NII).

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
8.	DoD 8570.01-M, Information Assurance Workforce Improvement Program	http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf	Provides guidance for the identification and categorization of positions and certification of personnel conducting Information Assurance (IA) functions within the DoD workforce supporting the DoD Global Information Grid (GIG) per DoD Instruction 8500.2. The DoD IA Workforce includes, but is not limited to, all individuals performing any of the IA functions described in this Manual. Additional chapters focusing on personnel performing specialized IA functions including certification and accreditation (C&A) and vulnerability assessment will be published as changes to this Manual.
9.	Joint Vision 2020	http://www.dtic.mil/doctrine/jel/jfq_pubs/1225.pdf	Strategic Guidance: Joint Vision 2020 builds upon and extends the conceptual template established by Joint Vision 2010 to guide the continuing transformation of America's Armed Forces.
10.	DoD Net-Centric Data Strategy	http://www.defenselink.mil/cio-nii/docs/Net-Centric-Data-Strategy-2003-05-092.pdf)	This Strategy lays the foundation for realizing the benefits of net centricity by identifying data goals and approaches for achieving those goals. To realize the vision for net-centric data, two primary objectives must be emphasized: (1) increasing the data that is available to communities or the Enterprise and (2) ensuring that data is usable by both anticipated and unanticipated users and applications. (Source: Department of Defense Net-Centric Data Strategy, DoD CIO, 9 May 2003
11.	DoD Net-Centric Services Strategy	http://dodcio.defense.gov/Portals/0/documents/DoD_NetCentricServicesStrategy.pdf	The DoD Net-Centric Services Strategy (NCSS) [R1313] builds upon the DoD Net-Centric Data Strategy's (May 2003) goals of making data assets visible, accessible, and understandable. The NCSS establishes services as the preferred means by which data producers and capability providers can make their data assets and capabilities available across the DoD and beyond. It also establishes services as the preferred means by which consumers can access and use these data assets and capabilities.
12.	DoD 5220.22-M, National Industrial Security Program Operating Manual	http://www.dss.mil/documents/odaa/nispom2006-5220.pdf	Provides baseline standards for the protection of classified information released or disclosed to industry in connections with classified contracts under the National Idustrial Security Program.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
13.	ICD 503, IT Systems Security, Risk Management, Certification and Accreditation	http://www.fas.org/irp/dni/icd/icd-503.pdf	This Intelligence Community Directive (ICD) establishes Intelligence Community (IC) policy for information technology systems security risk management, certification and accreditation. This ICD focuses on a more holistic and strategic process for the risk management of information technology systems, and on processes and procedures designed to develop trust across the intelligence community information technology enterprise through the use of common standards and reciprocally accepted certification and accreditation decisions.
14.	DoDD 8500.01E Information Assurance (IA)	http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf	Establishes policy and assigns responsibilities under reference (a) to achieve Department of Defense (DoD) information assurance (IA) through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare.
15.	DoDI 8500.2 - IA Implementation	http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf	Implements policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DoD information systems and networks
16.	DoD 8570.01, Information Assurance Training, Certification, and Workforce Management	http://www.dtic.mil/whs/directives/corres/pdf/857001p.pdf	Establishes policy and assigns responsibilities for Department of Defense (DoD) Information Assurance (IA) training, certification, and workforce management.
17.	DoDI 8510.01, Information Assurance Certification and Accreditation Process (DIACAP),	http://www.dtic.mil/whs/directives/corres/pdf/851001p.pdf	DoD Information Assurance Certification and Accreditation Process (DIACAP)
18.	DFARS 252.227-7014 RIGHTS IN NON-COMMERCIAL COMPUTER SOFTWARE AND NON-COMMERCIAL COMPUTER SOFTWARE	http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/dfars/Dfars252_227.htm#P696_47162	252.227-7014 Rights in technical data and computer software—small business innovation research (SBIR) program.
19.	DFARS 252.227-7017 Identification and Assertion of Use, Release, or Disclosure Restrictions	https://acc.dau.mil/CommunityBrowser.aspx?id=33760	Provides requirements for the identification and assertion of technical data.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
20.	Department of Defense Architecture Framework (DoDAF) Ver2.02 Aug 2010	http://dodcio.defense.gov/dodaf20.aspx	The Department of Defense Architecture Framework (DoDAF), Version 2.0 is the overarching, comprehensive framework and conceptual model enabling the development of architectures to facilitate the ability of Department of Defense (DoD) managers at all levels to make key decisions more effectively through organized information sharing across the Department, Joint Capability Areas (JCAs), Mission, Component, and Program boundaries. The DoDAF serves as one of the principal pillars supporting the DoD Chief Information Officer (CIO) in his responsibilities for development and maintenance of architectures required under the Clinger-Cohen Act. DoDAF is prescribed for the use and development of Architectural Descriptions in the Department. It also provides extensive guidance on the development of architectures supporting the adoption and execution of Net-centric services within the Department.
21.	Security Technical Implementation Guides (STIGs) CJCSI 6510.01F INFORMATION ASSURANCE (IA) AND SUPPORT TO COMPUTER NETWORK DEFENSE (CND)	www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf · PDF file	The Security Technical Implementation Guides (STIGs) and the NSA Guides are the configuration standards for DOD IA and IA-enabled devices/systems. Since 1998, DISA Field Security Operations (FSO) has played a critical role enhancing the security posture of DoD's security systems by providing the Security Technical Implementation Guides (STIGs). The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack. DISA FSO is in the process of moving the STIGs towards the use of the NIST Security Content Automation Protocol (S-CAP) in order to be able to "automate" compliance reporting of the STIGs.
22.	DODD 8100.1, Global Information Grid (GIG) Overarching Policy	http://www.acq.osd.mil/ie/bei/pm/ref-library/dodd/d81001p.pdf	Establishes policy and assigns responsibilities for GIG configuration management, architecture, and the relationships with the Intelligence Community (IC) and defense intelligence components.
23.	DODD 4630.05, Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)	http://www.dtic.mil/whs/directives/corres/pdf/463005p.pdf	Defines a capability-focused, effects-based approach to advance IT and NSS interoperability and supportability across the Department of Defense. Establishes the Net-Ready Key Performance Parameter (NR-KPP) to assess net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. The NR-KPP replaces the Interoperability KPP and incorporates net-centric concepts for achieving IT and NSS interoperability and supportability.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
24.	DoDI 5230.24, Distribution Statements on Technical Documents	http://www.dtic.mil/whs/directives/corres/pdf/523024p.pdf	This instruction updates policies and procedures for marking technical documents, including production, engineering, and logistics information, to denote the extent to which they are available for distribution, release, and dissemination without additional approvals or authorizations.
25.	DoDI 3020.37, Continuation of Essential DoD Contractor Services During Crises	http://www.afsc.army.mil/gc/files/i302037.pdf	This Instruction implements DoD policy, assigns responsibilities, and prescribes procedures, to provide reasonable assurance of the continuation of essential services provided by DoD contractors, including services provided to Foreign Military Sales (FMS) customers, during crisis situations.
26.	Cloud Computing / Department of Defense (DoD) Information Technology (IT) Enterprise Strategy and Roadmap	http://dodcio.defense.gov/Portals/0/Documents/Announcement/Signed_ITESR_6SEP11.pdf	In August 2010, the Secretary of Defense (SecDef) announced a Department of Defense (DoD)–wide Efficiencies Initiative to move America's defense institutions toward a ―more efficient, effective, and cost-conscious way of doing business.‖1 DoD Components were directed to conduct a ―zero-based review‖ of how they carry out their missions and of their priorities, and to rebalance resources to better align with DoD's most critical challenges and priorities. As part of the announcement, the SecDef directed consolidation of information technology (IT) infrastructure assets to achieve savings in acquisition, sustainment, and manpower costs and to improve DoD's ability to execute its missions while defending its networks against growing cyber threats.
27.	DoD Discovery Metadata Specification (DDMS 5.0, DoD Metadata Registry	https://metadata.ces.mil/dse/irs/DDMS/	The DDMS v4.1 schema is dependent on the DES for Information Security Metadata (ISM) version 9 and the DES for Need to Know (NTK) version 7. It also requires IC-Commons, which is distributed in the IRM version 7 distribution package.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
28.	AFI 33-138, Enterprise Network Operations Notification and Tracking	http://www.e-publishing.af.mil/shared/media/epubs/AFI33-138.pdf	This Air Force instruction (AFI) implements Air Force Policy Directive (AFPD) 33-1, Command, Control, Communications, and Computer (C4) Systems; the Information Assurance Vulnerability Management Program; and incident and vulnerability reporting guidance provided in Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND). This instruction prescribes and explains the various notification and tracking processes required to direct action and report status throughout the Air Force Network Operations (AFNETOPS) hierarchy. The specific processes addressed include Time Compliance Network Order (TCNO); Command, Control, Communications and Computers Notice to Airmen (C4 NOTAM); and incident, vulnerability, security incident, and service interruption reporting.
29.	AFI 61-204, Disseminating Scientific and Technical Information	http://www.dtic.mil/whs/directives/corres/pdf/523024p.pdf	This instruction updates the procedures for identifying export-controlled technical data and releasing export-controlled technical data to certified recipients and clarifies the use of the Militarily Critical Technologies List. It establishes procedures for the disposal of technical documents.
30.	AFI 33-119 Air Force Messaging	http://www.af.mil/shared/media/epubs/AFI33-119_AFDWSUP_I.pdf	AFI 33-119, Air Force Messaging is supplemented as follows. It outlines messaging services for 844 Communications Group customers. This supplement also establishes policy on individual (personal) and organizational mailboxes. It is applicable to all Bolling AFB and tenant units supported by the 844th Communications Group. Note: This supplement does not apply to squadrons assigned to the 844th Communications Group supporting the Pentagon (844 Communications Squadron) and Andrews Air Force Base (744 Communications Squadron).
31.	AFMAN 33-363, Management of Records	http://www.fas.org/irp/doddir/usaf/afman33-363.pdf	Guidance on Records Management

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
32.	AFI 33-115, Network Operations (NetOps), Vol 1	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-115v1/afi33-115v1.pdf	This Air Force instruction (AFI) implements Air Force Policy Directive (AFPD) 33-1, Command, Control, Communications, and Computer (C4) Systems (will become Information Resources Management). This instruction provides the overarching policy, direction, and structure for the Air Force Global Information Grid (AF-GIG) and procedures necessary to manage the increasingly complex network environment.
33.	AFI 63-101, Acquisition and Sustainment Life Cycle Management	http://static.e-publishing.af.mil/production/1/saf_aq/publication/afi63-101/afi63-101_20-101.pdf	It identifies elements of Air Force systems engineering (SE) practice and management required to provide and sustain, in a timely manner, cost-effective products and systems that are operationally safe, suitable, and effective.
34.	AFI 31-401, Information Security Program Managament	http://static.e-publishing.af.mil/production/1/af_a4_7/publication/afi31-401/afi31-401.pdf	This publication implements Air Force Policy Directive (AFPD) 31-4, Information Security. It prescribes and explains how to manage and protect unclassified controlled information and classified information. Use this instruction with Executive Order (EO) 12958, as amended, Classified National Security Information, 25 March 2003; Office of Management and Budget (OMB), Information Security Oversight Office (ISOO) Directive Number 1, Classified National Security Information, Executive Order 12829, National Industrial Security Program (NISP), DOD Manual 5220.22, National Industrial Security Program Operating Manual, January 1995; and, Department of Defense (DOD) 5200.1-R, Information Security Program, 14 Jan 97, for the management of the Air Force Information Security Program. Additional references include DOD Instruction (DODI) 5240.11, Damage Assessments, 23 Dec 91; DOD Directive (DODD) 5210.83, Unclassified Controlled Nuclear Information (UCNI), 15 Nov 91; Air Force Policy Directive (AFPD) 31-4, Information Security. This instruction is applicable to contractors as prescribed in AFI 31-601, Industrial Security Program. All these references are listed at the end of each paragraph where applicable. This instruction is not to be used as a stand-alone document. HQ USAF/XOS-F is delegated approval authority for revisions to this AFI.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
35.	AFPD 33-3, Information Management	http://www.fas.org/irp/doddir/usaf/afpd33-3.pdf	This policy directive establishes Air Force policy for the management of information assets (all forms of data and content), across all AF information sources, as both a strategic resource and corporate asset supporting the warfighter during mission and support operations.
36.	AFI 33-401, AIR FORCE ARCHITECTING	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-401/afi33-401.pdf	This Air Force Instruction (AFI) implements Air Force Policy Directive (AFPD) 33-4, Enterprise Architecting. This instruction describes the federation of Air Force architectures and its concept for federated architecture development, its associated business rules, governance, and the roles and responsibilities for appropriate Air Force organizations.
	AFI 31-501, Personnel Security Program Management	http://www.e-publishing.af.mil/shared/media/epubs/AFI31-501.pdf	Use this instruction with the DOD Regulation 5200.2-R and AFPD 31-5 to implement the personnel security program. This instruction requires collecting and maintaining information protected by the Privacy Act of 1974 authorized by Executive Orders 9397, 9838, 10450, 11652, and 12968; and 5 United States Code (U.S.C.) 7513, 7532, 7533; 10 U.S.C. 8013.
37.	AFI 33-332, Air Force Privacy Act Program	http://www.e-publishing.af.mil/shared/media/epubs/AFI33-332.pdf	Records that are retrieved by name or other personal identifier of a U.S. citizen or alien lawfully admitted for permanent residence are subject to Privacy Act requirements and are referred to as a Privacy Act system of records. The Air Force must publish SORNs in the Federal Register, describing the collection of information for new, changed or deleted systems to inform the public and give them a 30 day opportunity to comment before implementing or changing the system.
38.	Air Force Continuity of Operations (COOP) Program	http://www.e-publishing.af.mil/shared/media/epubs/AFI10-208.pdf	This Instruction implements Air Force Policy Directive (AFPD) 10-2, Readiness, and is consistent with AFPD 10-8, Homeland Security. It describes policy and requirements for implementing DODI 3020.42, Defense Continuity Plan Development, and DODI O-3020.43, Emergency Management and Incident Command of the Pentagon Facilities; DODI O-3000.08 Balanced Survivability Assessments (BSAs);and O-DODI 5110.11, Raven Rock Mountain Complex (RRMC).

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
39.	AFI 99-103, Capabilities-Based Test and Evaluation	https://acc.dau.mil/adl/en-US/509373/file/63688/OI002.pdf	It describes the planning, conduct, and reporting of cost effective test and evaluation (T&E) programs as an efficient continuum of integrated testing known as seamless verification. The overarching functions of T&E are to mature sys-tem designs, manage risks, identify and help resolve deficiencies as early as possible, and ensure systems are operationally mission capable (i.e., effective and suitable). The Air Force T&E community plans for and conducts integrated testing as an efficient continuum known as seamless verification in collaboration with the requirements and acquisition communities.
40.	AFI 33-114, Software Management	http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA404975	It identifies responsibilities for management of commercial off-the-shelf (COTS) and Air Force-unique software acquired by the Air Force. It includes policy and management structure for establishing and managing Air Force COTS software licenses and ensuring compliance with The Copyright Act and E.O. 13103.
41.	AFI 10-701, Operations Security (OPSEC)	http://www.e-publishing.af.mil/shared/media/epubs/AFI10-701.pdf	This publication provides guidance for all Air Force personnel (military and civilian) and supporting contractors in implementing, maintaining and executing OPSEC programs. It describes the OPSEC process and discusses integration of OPSEC into Air Force plans, operations and support activities.
42.	AFI 33-200, Information Assurance	http://afnafpo.com/pages/Doing-Business-With-AFNAFPO/AFNAFPOBusinessOpportunities/Docs/SecHill/6-AFI%2033-200%20Info%20Assurance.pdf	This AFI provides general direction for implementation of IA and management of IA programs according to AFPD 33-2. Compliance ensures appropriate measures are taken to ensure the availability, integrity, and confidentiality of Air Force ISs and the information they process. Using appropriate levels of protection against threats and vulnerabilities help prevent denial of service, corruption, compromise, fraud, waste, and abuse.
43.	AFI 33-210, AF Certification and Accreditation Program (AFCAP)	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-210/afi33-210.pdf	AF C&A program guidance
44.	AF Enterprise Architecture (AF EA) Compliance Guidance (Version 1.0 (final), December 2008	Located on X drive under engineering/Standards/Enterprise Architecture	The purpose of this document is to identify and document the Air Force Enterprise Architecture (AF EA) compliance criteria used to assess the degree to which each Air Force Information Technology (IT) system or National Security System (NSS), if applicable, conforms to existing AF enterprise guidance and requirements.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
45.	AFI 33-364, Records Disposition – Procedures and Responsibilities	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-364/afi33-364.pdf	Records Dispostion Procedures
46.	Air Force Program Executive Office (AFPEO) Business Enterprise Systems (BES) Systems Engineering Process	https://acc.dau.mil/bes	The Systems Engineering Process is a life cycle management and systems engineering process based on the Defense Acquisition, Technology, and Logistics Life Cycle Management System as tailored for Information Technology Systems and the Capability Maturity Model Integrated. It provides common plans, procedures, checklists, forms, and templates that support system life cycle management and systems engineering processes.
47.	AFI 10-601, Capabilities-Based Requirements Development	http://www.survivalebooks.com/free%20manuals/2006%20US%20Air%20Force%20CAPABILITIES%20BASED%20REQUIREMENTS%20DEVELOPMENT%2074p.pdf	The primary intent of this instruction is to facilitate timely development and fielding of affordable and sustainable operational systems needed by the combatant commander. The primary goal is to fulfill stated defense strategy needs with effects based, capabilities-focused materiel and non-materiel solutions. These solutions must be well integrated to provide suitable, safe, and interoperable increments of capability that are affordable throughout the life cycle.
48.	Air Force Policy Directive (AFPD) 33-4, Enterprise Architecting	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afpd33-4/afpd33-4.pdf	This directive establishes the AF policy for IT Governance to fulfill the AF CIO responsibilities established in federal laws and DoD issuances and the AF IT Governance Executive Board, which will oversee existing IT investment councils, boards, and working groups throughout the IT lifecycle to effectively and efficiently deliver capabilities to users. This directive focuses on aligning IT policy, CIO policy, and capabilities management with doctrine, statutory, and regulatory guidelines that govern accountability and oversight over IT requirements to resource allocation, program development, test, and deployment and operations under the direction and authority of the AF IT Governance Executive Board chaired by the AF CIO.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)

Standard		URL	Description
49.	AFI 33-115 Network Operations V1	http://static.e-publishing.af.mil/production/1/saf_cio_a6/publication/afi33-115v1/afi33-115v1.pdf	This AFI provides the overarching policy, direction, and structure for the Air Force-Global Information Grid (AF-GIG). It is a key component in the efforts to perationalize and Professionalize the Network (OPTN). The goal of Network Operations (NETOPS) is to provide effective, efficient, secure, and reliable information network services used in critical Department of Defense (DOD) and Air Force communications and information processes. This instruction provides the guidance necessary to manage the increasingly complex network environment and provide customers high quality services. Our networks have evolved into mission critical systems supporting Air Expeditionary Forces (AEF) and joint operations. Continued reliance on information-based weapons systems drives the need for a cohesive Air Force network.
50.	ANSI-J-STD-607-A, Commercial Building Grounding and Bonding Requirements for Telecommunications	http://www.tiaonline.org/	Must be purchased.
51.	TIA/EIA-TSB-72, Centralized Optical Fiber Cabling Guidelines (See comments)	http://www.tiaonline.org/	Must be purchased.
52.	TIA/EIA-TSB-75, Additional Horizontal Cabling Practices for Open Offices (See comments)	http://www.tiaonline.org/	Must be purchased.
53.	Netcentric Enterprise Solutions for Interoperability (NESI)	http://nesipublic.spawar.navy.mil/	NESI is a body of architectural and engineering knowledge that guides the design, implementation, maintenance, evolution, and use of the Information Technology (IT) portion of net-centric solutions for defense application.
54.	IEEE Standards	Too Broad	

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
55.	International Standards Organization (ISO)	http://www.iso.org/iso/home.html	ISO (International Organization for Standardization) is the world's largest developer and publisher of International Standards. ISO is a network of the national standards institutes of 162 countries, one member per country, with a Central Secretariat in Geneva, Switzerland, that coordinates the system. ISO is a non-governmental organization that forms a bridge between the public and private sectors. On the one hand, many of its member institutes are part of the governmental structure of their countries, or are mandated by their government. On the other hand, other members have their roots uniquely in the private sector, having been set up by national partnerships of industry associations. Therefore, ISO enables a consensus to be reached on solutions that meet both the requirements of business and the broader needs of society.
56.	ANSI/TIA/EIA-568-C, Commercial Building Telecommunications Cabling Standard	http://www.tiaonline.org/	The Telecommunications Industry Association (TIA) is the leading trade association representing the global information and communications technology (ICT) industries through standards development, government affairs, business opportunities, market intelligence and certification. With support from its 600 members, TIA enhances the business environment for companies involved in telecommunications, broadband, mobile wireless, information technology, networks, cable, satellite, unified communications, emergency communications and the greening of technology. TIA is accredited by ANSI.
57.	ANSI/TIA/EIA-569-1990, Commercial Building Standard for Telecommunications Pathways and Spaces	http://www.tiaonline.org/	Must be purchased.
58.	ANSI/TIA/EIA-606-A-ERTA, 2007, Administration Standard for the Telecommunications Infrastructure of Commercial Building	http://www.tiaonline.org/	Must be purchased.
59.	Federal Telecommunications Recommendation 1090-1997, Commercial Building Telecommunications Cabling Standard	http://www.ncs.gov/library/fed_rec/FTR%201090-1997.pdf	This recommendation specifies minimum requirements for telecommunications cabling within a building and between buildings in a campus environment. The specifications provide for a cabling system with a recommended topology and recommended distances, for copper and optical-fiber transmission media by parameters that determine performance, and for connectors and their pin assignments to ensure interconnectability. This recommendation is based on ANSI/TIA/EIA-568-A-1995, which replaces ANSI/EIA/TIA-568-1991 (FIPS PUB 174).

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
60.	AFI 33-580, Spectrum Management	http://www.e-publishing.af.mil/	This instruction establishes guidance and procedures for Air Force-wide management and use of the electromagnetic spectrum and implements Department of Defense Instruction (DoDI) 4650.01, Policy and Procedures for Management and Use of the Electromagnetic Spectrum; DoDI 8320.05, Electromagnetic Spectrum Data Sharing; National Telecommunications and Information Administration (NTIA) Manual of Regulations and Procedures for Federal Radio Frequency Management; Air Force Policy Directive (AFPD) 33-5, Warfighting Integration; and the procedures established by the Joint Staff J65A United States Military Communications-Electronics Board (USMCEB).
61.	AFI 33-111 Voice Systems Management	http://static.e-publishing.af.mil/production/1/934aw/publication/afi33-111_934awsup_i/afi33-111_934awsup_i.pdf	This instruction contains guidelines and procedures for managing Air Force voice systems and networks. Ensures installation, removal, modification, and relocation of telephone services are necessary to either sustain billing integrity, or to provide new service to offices/locations without base telephone service already present, or to maintain telephone numbers with primary offices that appear in the base telephone directory. Assure telephone services remain attached to organizations/functions versus individual personnel; do not submit requests to relocate telephone number(s) or telephone instrument(s) when personnel are assigned to a new office unless the reassignment is associated with an organizational restructure and the individual continues to perform the same organizational function. Otherwise, personnel transitioning to a new office will inherit the existing telephone number(s) and instrument(s) at the new location and update the Global Address Listing with their new telephone number(s). If no base telephone service is available at the new location, TCOs will submit a request to obtain service.

NETWORK OPERATIONS AND INFRASTRUCTURE SOLUTIONS (COMPLIANCE)			
Standard		URL	Description
62.	AFI 32-10112 Installation GI&S (GeoBase)	http://static.e-publishing.af.mil/production/1/af_a4_7/publication/afi32-10112/afi32-10112.pdf	This instructions convey guidance and procedures allowing commanders and Air Force professionals to maintain a flow of timely geospatial information with due regard for national security, accuracy, and privacy. Describe Geospatial Information and Services (GI&S) support for the installation and facilities mission, hereafter referred to as the GeoBase Program or GeoBase. Explain the organization and execution of the GeoBase Program for all levels of command. GI&S is the key platform for cross functional integration, and to that end this AFI provides guidance for those organizations seeking to integrate with the Geo-Base Service. Provide guidance and procedures for all Air Force military and civilian personnel that perform or utilize GeoBase functions, products or systems, including those in the Air National Guard and U.S. Air Force Reserve. This instruction is not intended to overlap or supersede GI&S guidance found in AFI 14-205, Geospatial Information and Services, 4 May 2004. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 37-123, Management of Records and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at https://afrims.amc.af.mil/. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

Appendix N4 - Market Research Template

Instruction: Perform your due diligence and complete your market research as it applies to your requirements. Note that it is not necessary to accomplish market research as it applies to available sources fit to perform the work. The contractors on the Network Operations and Infrastructure Solutions contract have been determined to be qualified to accomplish any requirements that fall within scope. Market research is performed IAW AFI 63-124 paragraph 1.4.2 and FAR Part 10. Include this document as part of your requirements package submitted to your Contracting Officer.

1. **DESCRIPTION OF SUPPLIES/SERVICES:** *(Describe the supplies or services to be acquired. Also state the anticipated lifecycle of the procurement (e.g., 1-yr base with four 1-yr option periods))*

2. **ACQUISITION HISTORY:** *(Describe previous contracts for the supplies/services described above, including previous subcontracting opportunities.)*

3. **CONDUCT OF THE RESEARCH:** *(Describe the steps taken and how the market research was conducted.*)

4. **MARKET RESEARCH FINDINGS:** *(Market Research for a specific requirement may be accomplished at the Solicitation level to determine what desired capabilities currently exist or are in development.)*

5. **DETERMINATION:**

Signed: ___________________________________ **Date:** ___________________

Appendix N5 - Quality Assurance Surveillance Plan (QASP) Templates

Instruction: This document provides a sample template for constructing a QASP for a Solicitation. Complete the template and include as part of the documentation submitted to the Contracting Officer (CO) for the requirements package. Notice the italic font provides supplemental instruction and sample language specific to each section. Delete all supplemental instruction and sample language before submitting to your CO. Please refer to AFI 63-124, paragraph 1.4.4, for additional guidance regarding development of a QASP.

1. **Solicitation Title:** [*Add Solicitation number at time of award]*

   Example: Mainframe Maintenance Service

2. **Requirements:** [List below the tasks specified in the PWS]

   Example:

   - Task 1 - Predictive/Preventive Maintenance
   - Task 2 - Equipment Repair
   - Task 3 - Dispatch Center
   - Task 4 - Work Documentation/Service Log Section
   - Task 5 - Equipment Monitoring Section
   - Task 6 - Configuration Management Section

3. **Primary Method of Surveillance:** (Choose a method that best fits your requirement, e.g., criticality of work to be performed, the relative importance of some tasks to others, lot size/frequency of service, surveillance period, stated performance standard, performance requirement, availability of agency people/resources, and cost-effectiveness of surveillance vs. task importance)

   Acceptable surveillance methods include:

   - ✓ **100 Percent Inspection.** This is usually only the most appropriate method for infrequent tasks or tasks with stringent performance requirements, e.g., where safety or health is a concern. With this method, performance is inspected/evaluated at each occurrence. One hundred percent inspection is too expensive to be used in most cases.

   - ✓ **Random Sampling.** This is usually the most appropriate method for recurring tasks. With random sampling, services are sampled to determine if the level of performance is acceptable. Random sampling works best when the number of instances of the services being performed is very large and a statistically valid sample can be obtained. Computer programs may be available to assist in establishing sampling procedures.

   - ✓ **Periodic Inspection:** These services are monitored weekly, monthly, quarterly, semiannually, annually, etc. Periodic types of activities are perfect for periodic inspection because not only are they infrequent, but there is normally a predetermined, specified time frame within which the tasks must be accomplished. Therefore, you know exactly when to conduct the evaluations. Periodic inspections automatically become 100 percent evaluations or "100 percent checks." Inspections should be divided and scheduled by frequency: annual, semiannual, quarterly, monthly, weekly and as required. Sometimes services are required for which the time or frequency cannot be predicted, such as accident investigations, one-time special tasking by higher headquarters, etc. These would be labeled "as required inspections." Others are known and predictable such as the quarterly status report or the monthly travel report currently included in some DISA service Solicitations.

- ✓ **Customer Input:** Although usually not a primary method, this is a valuable supplement to more systematic methods. For example, in a case where random sampling indicates unsatisfactory service, customer complaints can be used as substantiating evidence. In certain situations where customers can be relied upon to complain consistently when the quality of performance is poor, e.g., dining facilities, building services, customer surveys and customer complaints may be a primary surveillance method, and customer satisfaction an appropriate performance standard. In all cases, complaints should be documented, preferably on a standard form.

- ✓ **Contractor Self-Reporting:** Appropriate for tasks like system maintenance where the contractor can provide system records that document performance; for development projects, monthly reports can detail problems encountered.

4. **Scope of Performance**: (Provide the scope of the requirement as described in the PWS)

   Example: The contractor will provide remedial maintenance service on-site with problem resolution completed within the specified timeframe. Remedial maintenance is defined to include service, including parts replacement, as necessary to restore equipment that is in an inoperable or degraded condition to normal operating effectiveness. Equipment problems attributed to software malfunctions are excluded. The contract reference is Paragraph 2.

5. **Performance Standards:** (Insert the Performance Parameters from the Service Delivery Summary in the PWS)

   Example:

   - Mainframe processing availability must be 95% during the hours 0800 - 1600

   - Response times for maintenance calls should occur within 4 hours of placing a call

6. **Acceptable Quality Level (AQL**): (Must be realistic, stating the minimum standard, percentage of errors allowed, cost trade-offs, etc.)

   Example: The ACL for this project is 100% due to the critical support provided by mainframe operations.

7. **Evaluation Method:**

   Example: The contracting officer's technical representative (COTR) will document the time of verbal notification to the contractor. The COTR will document the official time and date of notification on the Maintenance Call Record. The COTR will review self-diagnostic systems logs, conduct a comparison with actual maintenance performance, and otherwise verify and validate contractor performance. The contractor shall enter in the record the official time the system is restored to full operational status. The COTR will confirm the date and time of problem resolution in the record.

8. **Incentives (Positive and/or Negative**): (Incentives should be used to encourage better quality performance and may be either positive, negative or a combination of both)

   Example: The following negative incentives apply in event of award to an OEM:

- If resolution is completed within 4 hours of notification, there will be no adjustment to the invoice amount.

- If resolution time exceeds 4 hours, the monthly invoice amount will be reduced by 10%.

Appendix N6 - Fair Opportunity Exception (FOE) Justification Template

Instruction: Complete this template if you are pursuing an exception to the fair opportunity process. Black italic font provides specific instruction for each respective section. Include this document as part of your requirements package submitted to the Contracting Officer. Depending on the dollar amount of the services requested, you will be required to complete one of the FOE Coordination and Approval templates contained in Appendix N11.

I. Contracting Activity

Fully identify the contracting activity responsible for the proposed contracting action. Include the name/phone number of the Contracting Officer. Specifically identify as an "Exception to Fair Opportunity" Justification. Identify purchase request number, if applicable. (NOTE: PR/Planning PR/Advanced PR must be attached to this exemption when sent for coordination/approvals)

II. Nature and/or Description of the Action Being Processed

State whether the action is a new order or by modification to an existing order. Identify the basic multiple award contract number and the order number for the current action. Also identify the type of the order/line items on the order (e.g., Firm Fixed price, Cost Plus Fixed Fee, etc.).

III. Description of the Supplies/Services Required To Meet the Agency's Needs

Specifically describe the supplies and/or services to be acquired including the price/cost and quantity of each item in the order and the total estimated value of the order. For services, state whether services are performance-based, and if not, provide rationale for not being performance based. Also state the delivery/performance schedule/period for the items under the order. (Note: The Contracting Officer must ensure that the order is issued within the period of performance and within the maximum value of the contract). Also explain how the requirement/order fits under the scope of the basic multiple award contracts.

IV. Authority Permitting a Fair Opportunity Exception

To assist you in preparing this justification, a sentence referencing the four exceptions to fair opportunity of FAR 16.505 (b)(2) are provided below. Include the following sentence in the justification with the appropriate exception inserted.

FAR 16.505(b)(1)(i) requires the Contracting Officer to provide each awardee under a multiple award contract, a fair opportunity to be considered for each order exceeding $3,000 unless a statutory exception applies. The specific exception that precludes the fair opportunity process for this acquisition is FAR 16.505(b)(2)(__) (Insert (i),(ii), (iii) or (iv), as applicable).

(Include the full text of the exception you are citing. Remove all others)

i. The agency's need for the services or supplies is of such urgency that providing such opportunity to all such contractors would result in unacceptable delays;

ii. Only one such contractor is capable of providing the services or supplies at the level of quality required because the service or supplies ordered are unique or highly specialized;

iii. The Solicitation should be issued on a sole source basis in the interest of economy or efficiency because it is a logical follow-on to an order already issued under DESP II, provided that all awardees were given a fair opportunity pursuant to the procedures in the above clause to be considered for the original order; or *iv. It is necessary to place an order to satisfy a minimum guarantee.*

V. Demonstration of the Contractor's Unique Qualifications or Nature of the Acquisition Requires the Use of the Authority Cited Above to Provide the Required Supply/Service (Applicability of Authority)

This section is normally the most detailed part of the justification. To assist you in preparing this justification, an introductory sentence for each of the FAR 16.505 (b)(2) exceptions to fair opportunity is provided below. Select the appropriate exception and provide in narrative form, a detailed explanation supporting the specific exception.

FAR 16.505(b)(2)(i), "The agency need for the supplies or services is so urgent that providing a fair opportunity would result in unacceptable delays". (When using this exception provide a detailed justification with supporting documentation that explains the exact urgency of the requirement and the mission impact if awarded to any other contractor. The user/customer typically provides this supporting information. Recommend attaching supporting documentation to the back of the document. General statements of urgency are not acceptable.)

FAR 16.505(b)(2)(ii), "Only one awardee is capable of providing the supplies or services required at the level at the level of quality required because the supplies or services ordered are unique or highly specialized". (When using this exception provide a detailed justification with supporting documentation, as evidence of the "unique or highly specialized" nature of the procurement. The user/customer typically provides this supporting information. Recommend attaching supporting documentation to the back of the document. General statements are not acceptable.)

FAR 16.505(b)(2)(iii), "The order must be issued on a sole-source basis in the interest of economy and efficiency as a logical follow-on to an order already issued under the contract, provided that all awardees were given a fair opportunity to be considered for the original order". (When using this exception provide information on the previously competed order under this contract and detail the economies and efficiencies that will be obtained by going sole source for the follow-on order. The user/customer typically provides this supporting information. General statements are not acceptable.)

FAR 16.505(b)(2)(iv), "It is necessary to place an order to satisfy a minimum guarantee."

VI. Description of Efforts Made To Ensure Competition Between All Awardees

(Recommended initial sentence for this section): In accordance with FAR 16.505(a)(1) orders under indefinite-delivery contracts do not have to be synopsized. Paragraph V, above, justifies why competition among all awardees is not possible for this acquisition. (Then discuss any actions taken to facilitate competition between all awardees for this acquisition. The discussion should include actions tried or considered even if the actions were unsuccessful. If the actions were unsuccessful, so state and describe why)

VII. Determination by the Contracting Officer That The Anticipated Cost to the Government Will Be Fair and Reasonable

The cost of this acquisition will be fair and reasonable. Actions anticipated to ensure reasonableness of the price will be accomplished with the procedures and criteria contained in the Federal Acquisition Regulation under Parts 30 – Cost Accounting Standards, and 31 – Contract Cost Principles and Procedures, and Subpart 15.4 – Contract Pricing, as appropriate. Further actions will be under the guidance of the Contract Pricing Reference Guides jointly developed by the Federal Acquisition Institute and the Air Force Institute of Technology. The AFMC Guide for Price Negotiation Memorandum/Price Competition Memorandum (PNM/PCM) will also be used , as *appropriate. Detailed documentation and justification of price reasonableness will be disclosed in the official PNM/PCM, to be prepared upon completion of negotiations*

VIII. Description of Market Research Conducted Among All Awardees and the Results Or A Statement of the Reason Market Research Was Not Conducted

Discuss the market research that was conducted by the user/technical team/contracting officer among the supplies/services of all awardees that resulted in the conclusion that a fair opportunity exception applied. The narrative in this section should provide a high level of confidence that the requirements of FAR 16.505(b)(1) and DFARS 216.505-70 could not be met. (Note: Since DFARS 216.505-70 has an additional fair notice/ fair opportunity requirement beyond that required by FAR 16.505(b)(1), the justification should also include a reference to DFARS 216.505-70.) If no market research was conducted, state so and provide the rationale.

IX. Other Facts Supporting the Justification

If the basic multiple award contract under which the order is to be placed is not a DoD contract, then Section 854 of the National Defense Authorization Act for FY2005 (P.L. 108-375) applies. Therefore, the justification should address how compliance with DFARS 217.78, Contracts or Delivery Orders issued by a Non DoD Agency, will be accomplished. (Note: DFARS 217.78 requires review and approval in accordance with agency procedures that the order is in the best interests of DoD). Provide any other facts supporting the use of the fair opportunity exception process.

X. List of Any Awardee That Expressed Interest in the Acquisition

If any other awardee expressed interest in fulfilling the requirement, but was not considered a potential source, explain why that awardee cannot provide the required supplies/perform the service.

XI. Actions the Agency May Take to Remove or Overcome Any Barriers To Increasing Fair Opportunity Before Any Subsequent Acquisition For the Supplies or Services

Describe all efforts to be to be taken to remove or overcome any barriers that preclude the agency from meeting the requirements of FAR 16. 505(b)(1) and DFARS 216.505-70 to provide competition between all awardees, before any subsequent acquisition for the supplies or services is made. If no actions are planned, so state and provide reasons

XII. Contracting Officer's Certification

The contracting officer's signature on the signature page evidences that he/she has determined this document to be both accurate and complete to the best of his/her knowledge and belief.

XIII. Technical/Requirements Personnel's Certification

As evidenced by their signatures on the signature page, the technical and/or requirements personnel have certified that any supporting data contained herein which is their responsibility is both accurate and complete.

Appendix N7 - Fair Opportunity Exception (FOE) Coordination & Approval Templates

TEMPLATE 1
COORDINATION AND APPROVAL PAGE
(>$0 but <$550,000.00)

Contracting Activity: _________________________

Purchase Request/Local Identification Number: _______________________________

Program Name (and Program Element, if applicable): __________________________

Estimated Cost/Price of the Order (including options): $__________________

Type Program: _______________________
Insert PEO Program or Other Contracting (see AFFARS 5302.101 for definitions)

Authority: FAR 16.505(b)(2)(__) (Insert (i),(ii),(iii) or (iv) , as applicable)

Type Determination: ____________________ **(Class or Individual)**

Solicitation Initiator: ________________________________ _____________
Preparer *(Name/Title)* Date Signed
DSN: Commercial:

Small Business Office: _______________________________ ______________
Coordination *(Name/Title)* Date Signed
(If required by the AOA) DSN: Commercial:

<u>Approval:</u>
Contracting Officer: __________________________ ______________
(Name/Title) Date Signed
DSN: Commercial:

TEMPLATE 2
COORDINATION AND APPROVAL PAGE
(>$550,000.00 but <$11,500,000.00)

Contracting Activity: _________________________

Purchase Request/Local Identification Number: _______________________________

Program Name (and Program Element, if applicable): __________________________

Estimated Cost/Price of the Order (including options): $__________________

Type Program: ________________________
Insert PEO Program or Other Contracting (see AFFARS 5302.101 for definitions)

Authority: FAR 16.505(b)(2)(__) (Insert (i),(ii),(iii) or (iv) , as applicable)

Type Determination: ____________________ (Class or Individual)

Solicitation Initiator: ____________________________ ______________
Preparer *(Name/Title)* Date Signed
DSN: Commercial:

Small Business Office: ____________________________ ______________
Coordination *(Name/Title)* Date Signed
(If required by the AOA) DSN: Commercial:

Contracting Officer: ____________________________ ________________
Coordination *(Name/Title)* Date Signed
DSN: Commercial:

Legal Office: ____________________________ _______________
Coordination *(Name/Title)* Date Signed
DSN: Commercial:

TEMPLATE 3
COORDINATION AND APPROVAL PAGE
(>$11,500,000.00 but <$78,500,000.00)

Contracting Activity: _________________________

Purchase Request/Local Identification Number: _______________________________

Program Name (and Program Element, if applicable): __________________________

Estimated Cost/Price of the Order (including options): $__________________

Type Program: ________________________
Insert PEO Program or Other Contracting (see AFFARS 5302.101 for definitions)

Authority: FAR 16.505(b)(2)(__) (Insert (i),(ii),(iii) or (iv) , as applicable)

Type Determination: ____________________ (Class or Individual)

Solicitation Initiator: __________________________ ________________
Preparer *(Name/Title)* Date Signed
DSN: Commercial:

Small Business Office: __________________________ ________________
Coordination *(Name/Title)* Date Signed
(If required by the AOA) DSN: Commercial:

Contracting Officer: __________________________ ________________
Coordination *(Name/Title)* Date Signed
DSN: Commercial:

Legal Office: __________________________ ________________
Coordination *(Name/Title)* Date Signed
DSN: Commercial:

Buying Office
Contracting Official: __________________________ ________________
Coordination *(Name/Title)* Date Signed
DSN: Commercial:

Competition Advocate: __________________________ ________________
Coordination *(Name/Title)* Date Signed
DSN: Commercial:

<u>Approval:</u>
Head of the Contracting
Activity: __________________________ ________________
(Name/Title) Date Signed
DSN: Commercial:

TEMPLATE 4
COORDINATION AND APPROVAL PAGE
(>$78,000,000.00)

Contracting Activity: ________________________

Purchase Request/Local Identification Number: ______________________________

Program Name (and Program Element, if applicable): _________________________

Estimated Cost/Price of the Order (including options): $_________________

Type Program: _______________________
Insert PEO Program or Other Contracting (see AFFARS 5302.101 for definitions)

Authority: FAR 16.505(b)(2)(__) (Insert (i),(ii),(iii) or (iv) , as applicable)

Type Determination: ___________________ (Class or Individual)

Solicitation Initiator: Preparer	__________________________ *(Name/Title)* DSN:	 Commercial:	_______________ Date Signed
Small Business Office: Coordination (If required by the AOA)	__________________________ *(Name/Title)* DSN:	 Commercial:	_______________ Date Signed
Contracting Officer: Coordination	______________________ *(Name/Title)* DSN:	 Commercial:	_______________ Date Signed
Legal Office: Coordination	______________________ *(Name/Title)* DSN:	 Commercial:	_______________ Date Signed
Buying Office Contracting Official: Coordination	________________________ *(Name/Title)* DSN:	 Commercial:	_______________ Date Signed
Competition Advocate: Coordination	________________________ *(Name/Title)* DSN:	 Commercial:	_______________ Date Signed
Senior Center Contracting Official: Coordination	________________________ *(Name/Title)* DSN:	 Commercial:	______________ Date Signed
Approval: Senior Procurement Executive of the Agency:	______________________ *(Name/Title)* DSN:	 Commercial:	_______________ Date Signed

Appendix N8 - DD Form 254 Guidance

1. The initial DD Form 254 is called a draft DD Form 254. A draft DD Form 254 is prepared by the program office for each contract involving classified information. The Contracting Officer (CO), the Industrial Security Program Manager (ISPM), and other security disciplines (i.e. AF security manager, Communications Security (COMSEC), SCI and Non-SCI Intelligence, and Operations Security (OPSEC)) or functional OPRs affected under the terms of the solicitation should be consulted when preparing the draft DD Form 254 to ensure accuracy. The program office coordinates contractual security specifications with the contracting office and responsible security discipline, office of primary responsibility (OPR) or functional.

2. Once the draft DD Form is completed, it is forwarded to the CO for processing.

3. The CO reviews and coordinates the draft DD Form 254 along with all affected security disciplines. Coordination (includes the office symbol, date, and initials of the reviewer) is annotated in block 13 of the draft DD Form 254. Coordination is completed in the following order (as necessary):

    a. AF Security Manager
    b. COMSEC
    c. SCI and Non-SCI Intelligence
    d. Foreign Disclosure
    e. OPSEC
    f. ISPM

1. After the draft DD Form 254 is reviewed and the required coordination is received, the CO returns it to the requesting AF program office. The CO maintains a copy of the annotated draft DD Form 254 in the respective contract file.

2. The program office receives the draft DD Form 254 and incorporates the necessary changes. Once all the recommended changes have been made, the program office prepares and forwards and original DD Form 254 to the CO for approval and signature.

3. The CO receives the original DD Form 254 and verifies all affected security disciplines and OPRs have reviewed and coordinated on the draft DD Form 254.

4. The CO ensures the ISPM reviews the draft and the original DD Form 254 (ISPM only coordinates on the draft DD Form 254).

5. The CO certifies the DD Form 254 by signing in block 16e.

6. Distribution:

    a. Procuring Contracting Officers (PCO) or their designated representatives are responsible for distributing the original DD Form 254 to the to the required distribution listed in blocks 17a-17f in addition to the security offices annotated in block 13 of the draft DD Form 254.

    b. If performance will occur on AF installation, the CO will provide a signed copy of the original DD Form to the ISPM at that location.

Appendix N9 - Inherently Governmental Functions Memo Template

Instruction: Since services are being required therefore a determination must be made by the Program Office certifying that there are no Inherently Governmental Functions (IGF) being accomplished by the Contractor. Complete the following memorandum certifying as such and include as part of your requirements package submitted to your Contracting Officer (CO). Refer to FAR Subpart 7.5, Inherently Governmental Functions, for further guidance and/or clarification.

DATE

MEMORANDUM FOR [organization name]

FROM: [name, organization]

SUBJECT: Inherently Governmental Functions Determination

The contractor will not perform any inherently governmental duties.

____

Title of Letter Preparer

Appendix N10 - Government Furnished Property Determination and Findings Template

Department of the Air Force

Name of Program

Determination and Findings

Government Furnished Property

Findings

1. Explain/Demonstrate why Government Property should be issued to Contractors using FAR 45.102 policy as your guide.

FAR 45.102 Policy

(b) Contracting officers shall provide property to contractors only when it is clearly demonstrated—

1) To be in the Government's best interest;

2) That the overall benefit to the acquisition significantly outweighs the increased cost of administration, including ultimate property disposal;

3) That providing the property does not substantially increase the Government's assumption of risk; and

4) That the Government requirement cannot otherwise be met.

Determination

1. The type of work that needs to be performed under this acquisition is of such a nature that….

2. Therefore, based on the findings and determination above, and pursuant to the authority of FAR 45.102, the proposed effort (name program) described above requires Government Furnished Property.

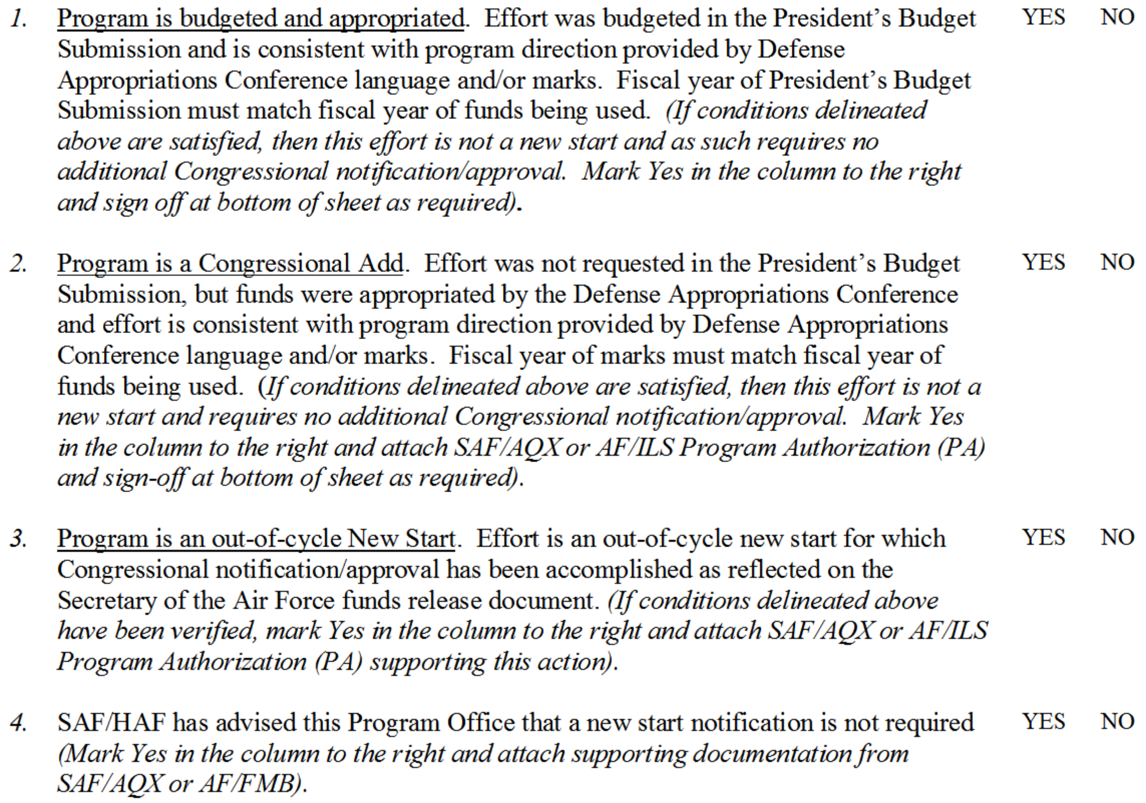
____________________________ ________________________________

Program Name Program Manager Date

Appendix N11 - New Start Validation Template

Instruction: Complete the following form and include as part of your requirements package submitted to your Contracting Officer (CO) if a new start program/project is applicable.

In accordance with AFI 63-101, I have reviewed AFI 65-601 & DoD FMR Vol III Chap 6 and confirmed the following prior to approving this action (one of the following must be answered yes and acknowledged (signed-off) by the Program Manager and Program's Chief Financial Officer (CFO) or Program Control Chief): If not a single item can be checked off as a YES, then the Program Office shall contact their respective PEM/CD at the HAF as delineated in CH 2, Par 2.3.1 of this AFI in order to being/coordinate New Start Notification package



1. Program is budgeted and appropriated. Effort was budgeted in the President's Budget Submission and is consistent with program direction provided by Defense Appropriations Conference language and/or marks. Fiscal year of President's Budget Submission must match fiscal year of funds being used. *(If conditions delineated above are satisfied, then this effort is not a new start and as such requires no additional Congressional notification/approval. Mark Yes in the column to the right and sign off at bottom of sheet as required)*. YES NO

2. Program is a Congressional Add. Effort was not requested in the President's Budget Submission, but funds were appropriated by the Defense Appropriations Conference and effort is consistent with program direction provided by Defense Appropriations Conference language and/or marks. Fiscal year of marks must match fiscal year of funds being used. (*If conditions delineated above are satisfied, then this effort is not a new start and requires no additional Congressional notification/approval. Mark Yes in the column to the right and attach SAF/AQX or AF/ILS Program Authorization (PA) and sign-off at bottom of sheet as required).* YES NO

3. Program is an out-of-cycle New Start. Effort is an out-of-cycle new start for which Congressional notification/approval has been accomplished as reflected on the Secretary of the Air Force funds release document. *(If conditions delineated above have been verified, mark Yes in the column to the right and attach SAF/AQX or AF/ILS Program Authorization (PA) supporting this action).* YES NO

4. SAF/HAF has advised this Program Office that a new start notification is not required *(Mark Yes in the column to the right and attach supporting documentation from SAF/AQX or AF/FMB).* YES NO

________________________________ ________________________________
Program Manager (Name/Grade) Date

________________________________ ________________________________
CFO/Program Control Chief (Name/Grade) Date

Department of Defense Appropriations Act 2000, Public Law 106-79 Sec. 8096. None of the funds in this Act may be used to compensate a DoD employee who initiates a New Start program without notification to OSD and the Congressional Defense Committees, as required by DoD financial management regulations.

Appendix N12 - Independent Government Cost Estimate

An Independent Government Cost Estimate (IGCE) is a necessary component of the requirements package submitted to the Contracting Officer. The information contained within this document serves as a guide to develop reliable, detailed cost estimates.

The IGCE is a procurement sensitive document and should be marked and handled accordingly. Access to the IGCE is on a need to know basis.

The three most common methodologies for estimating costs of IT and netcentric requirements are: (1) Analogy, (2) Tools Using Parametric Models, and (3) Engineering Buildup otherwise referred to as the Bottoms-Up Methodology. A best practice is to use both a primary methodology and a secondary methodology as a cross-check.

1. **Analogy**
   This method relies on similarities between proposed and historical tasks and projects. It requires the collection of information from historical tasks which appear to be comparable in nature to the proposed tasks. The effectiveness of this method depends heavily on the ability to correctly identify similarities between tasks, thus providing the ability to project reliable, accurate estimates.

2. **Tools Using Parametric Models**
   There are commercial products available such as SEER (i.e., SEER-SEM, SEER-IT), Cost Xpert, and Constructive Cost Model (COCOMO) that are used as estimation methods of IT projects and software development for effort, schedule, resources, and maintenance costs as a function of size, technology, and any project management constraints. Most of these products are based on sound science and draw from applicable project histories, which when combined with parametric modeling techniques produces cost-estimate relationships for various elements of Solicitation requirements. A free version of the COCOMO software tool is available at **cocomo**-ii-application-for-software-cost-estimation.soft32.com.

3. **Engineering Buildup / Bottoms-Up Methodology**
   This method is performed at the lowest possible level of detail and uses industrial engineering techniques, such as time standards, to develop the estimate by summing the detailed estimates done at low level work breakdown structure (WBS) levels. Typically, the cost estimator works with engineers and/or Subject Matter Experts (SMEs) familiar with the tasks being estimated. The experience accumulated can constitute a large knowledge base from which to assess the resources needed for a specific task. This experience is often translated into 'rules of thumb' for reliable cost estimates. The preference is to use objective relevant historical data as the basis of estimate or to validate the expert judgment from engineers/SMEs. Note, it is best to accomplish this methodology in a spreadsheet, a sample format is provided below.

Other cost estimating methods include: expert opinion, which relies on SMEs to give their opinion on what an element should cost; and extrapolating, which uses actual costs and data from previous work and/or prototypes to predict the cost of future elements.

Steps to a High-Quality IGCE Process		
Step	**Description**	**Associated Task**
1.	Define estimate's purpose	An IGCE is conducted to serve as an objective basis for determining whether a contractor's cost proposal is fair and reasonable and to make sure that the offered prices are within the budget range of the program for this particular contract effort. It is based on contract requirements (PWS) and is developed without the influence of potential contractors' efforts. While independence from contractor inputs is required, the IGCE should be prepared from a contractor's point of view, required level of detail and scope. Will it require a risk confidence level?
2.	Develop estimating plan	Ensure appropriate estimating team is in place (e.g., cost estimator(s), engineers, Subject Matter Experts (SMEs). Consult your Financial Management office for cost estimating support for complex estimates. Schedule your estimate timeline to coincide with the acquisition schedule need dates. Consider estimate methodologies.
3.	Define program characteristics	Ensure all PWS requirements are understood and captured in the IGCE and nothing outside the PWS is included. Remember you're building the IGCE from a contractor's point of view. If you don't understand the requirements as a Gov't analyst, it's likely they won't either, especially non-incumbents. Your acquisition schedule and strategy will impact the level of detail and format for your IGCE. Identify relationship of this effort to other existing systems or predecessor effort. Identify quantities, size inputs.
4.	Develop estimating structure	Develop a Work Breakdown Structure (WBS) or cost element structure. Make sure the IGCE is at least the same level of fidelity as the contract structure. If there are multiple contract line item numbers (CLINs), then your IGCE should be broken out by CLIN. Choose the best estimating method for each WBS cost element and look for potential cross-checks and schedule drivers.
5.	Identify ground rules and assumptions	Clearly define what the estimate includes and excludes. Identify inflation tables used; contract period of performance (PoP) by base and option periods; projected milestones such as IOC, FOC; technology refresh cycles, etc.
6.	Obtain data	Look for current, relevant technical, programmatic, cost and risk data. Normalize the data for cost accounting, inflation, learning and quantity adjustments. Analyze the data for cost drivers, trends and outliers and compare results against rules of thumb and standard factors derived from historical data.
7.	Develop IGCE	Develop the cost model estimating each WBS element with the best methodology from the data collected. IGCE costs will be presented in then-year costs. Perform cross-checks on key cost drivers.

Steps to a High-Quality IGCE Process		
Step	**Description**	**Associated Task**
8.	Conduct risk and uncertainty analysis	If your IGCE is going before an ASP, a risk confidence level will be requested. This entails discussing with SMEs the level of cost, schedule and technical risk associated with each WBS element. Develop minimum, most likely and maximum ranges for each risk element and use a cost model like ACE-IT or Crystal Ball to develop a confidence level distribution. Identify risk dollars required over and above the point estimate to fund to the desired confidence level.
9.	Document the estimate	Document all steps used to develop the estimate so that an independent analyst could replicate the results. AFI65-508 details documentation standards.

IGCE Best Practices:

- **<u>Form a Team Early</u>:** Assemble a team of stakeholders and experts as soon as practical. Get the person(s) doing the cost analysis involved in your acquisition program and development of the IGCE.

- **<u>Use a Structured Approach</u>:** Define and document a structured approach to size your acquisition [Work Breakdown Structure (WBS), Cost Element Structure (CES), models, analogies with other acquisitions, market survey plans, etc., or combinations of these]. This structure provides the baseline for many acquisition decisions.

- **<u>Tailor IGCEs from Standard Formats</u>:** Information is important, format is of lesser importance. Most acquisitions call for unique combinations. These do not lend themselves to a single standardized format. Use a logical approach and standard spreadsheets or common application software that allows IGCEs to be easily developed and transferred electronically.

- **<u>Include standard program information and coordination:</u>**

    - Program Title
    - Action Officer (Acquisition Manager)
    - Phone/E-mail address
    - IGCE Preparer/Phone/Signature/Date
    - Resource Manager/Phone

- **<u>Use standard cost elements (tailored to fit the acquisition):</u>**
    - Direct Labor Cost (DLC)
    - Other Direct Costs (ODC): Materials & Supplies, Equipment, Travel, IT, Other
    - Overhead Costs (OVHD)
    - General & Administrative Costs (G&A)
    - Profit (Fee)

- **<u>Ensure "independence" through market research</u>:** Using price/cost data from a single contractor, without scrutiny, invalidates the "independence" that makes your IGCE useful in contract negotiations. From a practical point of view, a single contractor's price lists, labor estimates, and other cost information are going to be used, but they are not supportable without a comparison to cost estimates of similar requirements identified in market research. Even unique requirements and sole source acquisitions require research into previous contracts, similar requirements, and the use of technical judgment to ensure that the data in the IGCE is unbiased.

- **Use "burdened" labor rates if possible:** These rates typically represent recently competed and negotiated rates for a large range of skills supporting information technologies. Using these burdened rates greatly simplifies the cost estimation process and format. Accuracy depends on the availability of burdened labor rates similar to the labor skills required in your acquisition.

- **Disparity between the offeror's price/cost and the IGCE may be a "Red Flag":** Differences greater than 25% between the offered price/cost and the IGCE may indicate a serious disconnect between what is being offered and the requirement. If the IGCE is revised, the revision should be documented.

Sample IGCE Format

	CLIN*	COST ELEMENT**	Direct Labor Category	Hours	Rate (Cost/Hr)	Total
	0001					
A.		1.Requirements				
			Program Mgr	1,000	$25.00	$25,000
			Software Eng	2,000	$22.50	$45,000
			etc.	2,000	$15.00	$30,000
		2. Design	Break out by Category like above	11,000	$20.00	$220,000
		3. Coding	"	17,000	$20.00	$340,000
		4. Testing	"	17,000	$20.00	$340,000
A.1		Total Direct Labor				$1,000,000
B.		Labor Burden (e.g. 35%) (A.1 x Burden Rate Factor)				$350,000
C.		Other Direct Costs				
		Supplies				$0
		Rentals				$0
		Travel				$10,000
D.		Subtotal - Direct Costs (A.1 + B + C)				$1,360,000
E.		Overhead (e.g. 10%) (OH Factor x D)				$136,000
F.		Subtotal				$1,496,000
G.		G&A (e.g. 15%) (G&A Factor x F)				$224,400
H.		Profit or Fee (e.g. 10%) (Profit/Fee Factor x [F + G])				$172,040
I.		Total Estimated CLIN Contract Price (sum F through H)				$1,892,440
	0002, etc.	Repeat above breakout for each contract CLIN				

Subcontractor direct labor expenses would have a Material & Handling (M&H) factor added, but no labor burden, overhead or G&A. Profit or fee is added to subcontractor DL and M&H

* Regardless of estimating methodology, your estimate should be aligned with your contract CLIN structure. Additionally, if your contract has a base period and options, each PoP should be broken out in the estimate

**For the engineering buildup, your estimate will be broken into lowest WBS direct cost elements (e.g., requirements, design, code). This level of detail is required documentation to support this methodology but it is not typically presented in the IGCE results for comparison to contractor proposals.

If your contract strategy allows for price analysis vice cost analysis, you will not have the breakout of individual cost elements (DL, overhead, G&A, profit) and the format above would utilize fully burdened rates vice the cost element breakout above.

Appendix N13 - Evaluation Guidelines

1. **Background.** The NETCENTRIC contracts were evaluated IAW FAR Subpart 15.3, which is a formal, prescribed process. The NETCENTRIC Solicitations do not have to go into as much detail. This is true because the contractors that have been awarded contracts under NETCENTRIC are qualified to accomplish the scope of work covered under this contract.

2. **Contracting Guidance.** Issuance of a Solicitation award will be made to the offeror whose offer conforms to the Performance Work Statement and provides the best value to the Government as identified in each individual Request for Proposal. The competition requirements in FAR Part 6 and the source selection requirements in FAR Subpart 15.3 do not apply to the ordering process; however, users shall follow the ordering procedures outlined in FAR 16.505, DFARS 216.505, and any other applicable supplements (i.e., mandatory procedures and informational guidance).

- ***Note that FAR 16.505(b)(3) addresses pricing, FAR 16.505(b)(5) addresses decision documentation, and both FAR 16.505(b)(1)(iv) and 16.505(b)(4) address specific requirements for Solicitations exceeding $5 million.***

3. **Evaluation Methodologies:**

There are three established methodologies for USAF evaluation of proposals:

1. Full Trade Off (FTO)
2. Lowest Price Technically Acceptable (LPTA)
3. Performance Price Tradeoff (PPT)

All of the methodologies use some combination of technical worthiness, price or past performance for evaluation. It's important to ensure that the selected methodology matches the requirements of the Solicitation. ***NOTE: LPTA and PPT do not rank the order of technical worthiness, and therefore are not ideal candidates for evaluation of technically complex requirements***. For more information on PPT and LPTA methodologies, visit the following link and navigate to Section 11.3. Best Value

4. **Examples:**

The requiring activity may also opt to state the evaluation in such simple or complex terms as the following examples:

a. The Government will select the proposal found to be most advantageous to the Government, price and other factors considered. Technical capability will be evaluated and is more important than price. Technical capability is defined as …(insert customer capabilities and/or standards – such as "tools, methodologies, and approach" to meet the requirements of the PWS).

b. The Government will select the proposal found to be most advantageous to the Government, price and other factors considered. In addition to price, technical capability and quality/past performance will be evaluated, and each factor is equally important.

c. The evaluation criteria are divided into factors and sub-factors. The offeror's response must demonstrate a clear understanding of the nature of the requirement. Each offeror's response will be evaluated against the criteria defined within the following areas in descending order of importance: (list the factors in order of importance)

d. The following evaluation criteria are divided into three factors: Mission Capability, Past Performance and Cost/Price.

1. Mission Capability

Mission Capability includes three parts, Technical Approach, Management Approach, and Risk.

a) Sub-Factor 1: Technical Expertise

- Familiarity in planning and installing networking software in classified/unclassified environment according to Air Force and DoD requirements
- Expertise in the field of software implementation
- Proper personnel mix of technical personnel, proper certifications/experience with tool proposed
- Ability to develop system management processes and procedures and apply at base/organization level
- System engineering process expertise

b) Sub-Factor 2: Management Approach

- Capability to manage contract project efforts
- Capability to convey accurate and timely project status
- Capability to efficiently manage large scale software implementation
- Proposed Processes for communication with government

c) Sub-Factor 3: Risk

- Schedule
- Cost
- Performance

2. Past Performance

The contractor shall provide a detailed description of the proposed team's experience on three efforts of similar content and scope, to include scope and outcome of the project(s). The past performance references must include a Government or Commercial Point of Contact information to include name, organization, title, e-mail address, mailing address, and phone number. Factors influencing past performance include:

- Experience on earlier orders under the IDIQ contract
- Experience on similar tasks of the same scope
- Past performance in meeting schedules
- Past performance in delivering high quality systems/services

NOTE, how to leverage ID/IQ past performance data?

3. Cost/Price

Cost/Price will be evaluated for reasonableness and completeness. Other than for a Firm Fixed Price order, the cost proposal should provide supporting cost data to include labor categories, labor rates, labor hours, other direct charges, and overhead rates.

Customers have the discretion to determine their needs and the best way(s) to meet them. Accordingly, there is broad discretion in the selection of the evaluation criteria used in acquisitions along with the weight/order of importance of those criteria/factors provided the criteria used reasonably relate to the customer's needs in selecting the contractor(s) that will best serve their interests. When required by the ordering procedures outlined in FAR 16.505, evaluation criteria will be identified and ranked for each individual RFP.

Appendix N14 - Ozone Depleting Substance Certificate

Instruction: Confirm whether or not the services required of this task award will require the contractor to use Class 1 Ozone Depleting Chemicals. Obtain the required signature(s) and include this certificate as part of the requirements package submitted to your Contracting Officer (CO).

In accordance with AFFARS 5323.803(b), I have reviewed the requirements, including available technical documentation, and believe that it does not require the contractor to use Class 1 Ozone Depleting Chemicals (ODCs) identified in Air Force Instruction 32-7086 Chapter 4 in performance of the contract, nor does it require the delivery of the Class 1 ODCs in any item of supply or as part of any service.

Program Manager or Functional Director　　　　　　　　　　Date